Univerzita Karlova
Pedagogická fakulta
Katedra informačních technologií a technické výchovy

BAKALÁŘSKÁ PRÁCE

Rizika sociálních sítí pro děti a mládež
The risks of social networks for children and youth

Miloš Hoznauer

Vedoucí bakalářské práce: Ing. Bořivoj Brdička, Ph.D.

Studijní program: BC-VYCH Vychovatelství

Studijní obor: Vychovatelství

2017

Prohlašuji, že jsem bakalářskou práci na téma *Rizika sociálních sítí pro děti a mládež* vypracoval pod vedením vedoucího práce samostatně za použití v práci uvedených pramenů a literatury. Dále prohlašuji, že tato práce nebyla využita k získání jiného nebo stejného titulu.

V Praze dne 20. dubna 2017

……

podpis

PODĚKOVÁNÍ: Děkuji tímto panu Ing. Bořivojovi Brdičkovi, Ph.D. za odborné vedené mé bakalářské práce.

ANOTACE

Bakalářská práce se zabývá riziky spojenými s užíváním internetu respektive sociálních sítí s důrazem na děti a mládež. Cílem této práce je zpracování kriminálních případů z vlastní policejní praxe a dalších známých i méně známých kauz, které se týkají této problematiky. Na základě analýzy těchto případů a odborných výzkumů byl vytvořen přehled existujících rizik užívání sociálních sítí. Po vyhodnocení zjištěných rizik byla vyhotovena metodická doporučení pro preventivní bezpečné chování v kyberprostoru i řešení konkrétních krizových situací.

V teoretické části jsou nejprve vysvětleny základní pojmy. V praktické části je rozebrán soubor zahraničních výzkumů a výzkum tuzemský, ve kterých jsou identifikována existující rizika. V další části je na tato rizika navázáno analýzou reálných kriminálních případů. Dále jsou popsány dostupné možnosti pomoci, které jsou společně s prevencí zapracovány do podoby metodických doporučení.

KLÍČOVÁ SLOVA

Sociální sítě, podvodné jednání, kyberšikana, kybergrooming, sexting, reálné kriminální případy, prevence, bezpečné a rizikové chování, online podpora, linka pomoci

ANNOTATION

The bachelor thesis describes the risks related to the use of internet, respectively social sites with focus on children and youth. The aim of the work to evaluate of criminal cases from my police experience and some more or less famous cases concerning this topic. Based on analysis of these cases and research reports, a list of risks of social network usage was created. After evaluation of the risks found, methodical recommendations for precautionary safe behavior in cyberspace and for dealing with real crisis situations were made out.

Firstly, the basic terms are explained in the theoretical part. In the practical part, an analysis of the foreign and domestic research reports was performed, where the existing risks were identified. The following part is connected by the analysis of the real criminal cases. Furthermore, the available help possibilities are described, which are integrated, together with the prevention, into the methodical recommendations.

KEYWORDS

Social networks, fraudulent act, cyberbullying, cybergrooming, sexting, real criminal cases, prevention, safe and risky behavior, online help, help line.

Obsah

1. Úvod

Když jsem si vybíral téma bakalářské práce, neměl jsem moc těžký výběr. Vybral jsem si téma, ve kterém jsem mohl propojit zkušenosti získané prací jako policista místního oddělení a znalostí nabytých studiem oboru vychovatelství. Rizika sociálních sítí pro děti a mládež jsem zvolil taktéž proto, že je toto téma v dnešní době o to víc aktuální, čím více dochází k používání výpočetní techniky, internetu a právě sociálních sítí. Na internetu číhá nebezpečí na všechny bez rozdílu pohlaví či věku, avšak děti a mládež jsou díky určité naivitě, absenci životních zkušeností a malé informovanosti ohroženy nejvíce. Touto prací bych to rád alespoň částečně změnil.

Když jsem v roce 2014 nastupoval na stáž na oddělení analytiky a informační kriminality služby kriminální policie a vyšetřování na Obvodním ředitelství policie Praha IV, obdržel jsem od kolegy, který mě školil, jeho bakalářskou práci, kterou měl na téma Problematika odhalování a vyšetřování kybernetické kriminality. Sloužila pro mě jako jakýsi manuál, ve kterém jsem se mj. mohl dočíst, na jakém principu funguje internet, jak probíhá emailová komunikace a jak odhalit pachatele například vyhrožování či majetkové trestné činnosti. Myšlenka následného využití bakalářské práce mi přišla velice přínosná a užitečná, s možností využití pro velký okruh čtenářů, od dětí, přes pedagogické pracovníky a rodiče až po příslušníky policie. Proto jsem se i já rozhodl vytvořit bakalářskou práci, která nebude sloužit jen k zakončení bakalářského studia, ale bude mít, jak doufám, dalšího využití.

V roce 1998 se moje nevlastní sestra s celou svojí početnou rodinou přestěhovala z Prahy do lázeňského města Jáchymov v okrese Karlovy Vary. Její manžel, akademický architekt, ke své práci nutně potřeboval počítač. Jáchymov v té době měl přibližně 2500 obyvatel, ale podle neoficiálních informací měl švagr jen jeden ze tří osobních počítačů, které se nacházely v domácnostech ve městě. Proto před domem stály doslova fronty (zejména dětí), aby si mohly počítač alespoň vyzkoušet. V té době totiž nebyly ještě osobní počítače v domácnostech tak finančně dostupné. Stály často i šest průměrných měsíčních platů. Internet byl ještě v roce 1995 spíše akademickou záležitostí. Podobná situace byla i na poli mobilních telefonů. Přístroje měly s trochou fantazie velikost a tvar armádních vysílaček a byly taktéž pro běžné lidi málo dostupné. Například já osobně jsem si svůj první mobilní telefon koupil až v roce 2000. Se vzrůstající nabídkou výpočetní techniky, mobilů a internetu, snižující se cenou techniky i služeb a tím pádem zvyšující se dostupností, se zvyšoval počet osobních počítačů a mobilních telefonů nejen ve firmách, ale i v domácnostech. Zároveň se neustále snižuje věk

dětí, kterým rodiče koupí mobilní telefon. Je to spíše z bezpečnostních důvodů, aby měli o dětech přehled, aby s nimi byli ve spojení, avšak děti na mobilních telefonech hrají hry a můžou se připojovat na internet a přistupovat tak na sociální sítě. V současné době disponuje téměř každá domácnost osobním počítačem s přístupem k internetu. S velkým rozmachem výpočetní techniky a internetu roste i nebezpečí jejího zneužití, co se týče nejen majetkové trestné činnosti, ale i k páchání například kyberšikany, kybergroomingu či ke zneužití dítěte k výrobě pornografie, v nejhorším možném případě může vše skončit i násilnou smrtí oběti.

Jelikož jedním z problémů, kterému se budu níže taktéž věnovat, je špatná znalost některých pojmů týkající se výpočetní techniky, sociálních sítí a jejich fungování ze strany dospělých, budou zde ze začátku, pro lepší informovanost a vhled do tématu, popsány základní pojmy, jako jsou internet, sociální sítě apod. Dále budou vyjmenovány nejpoužívanější sociální sítě a popsána jejich charakteristika a primární účel. Nakonec bych se věnoval hlavním pojmům možného zneužití na internetu respektive na sociálních sítích. V praktické části se budu věnovat rozboru dvou rozsáhlých výzkumů, a to jednomu tuzemského a souboru několika zahraničních výzkumů v rámci jednoho projektu EU KIDS ONLINE, a to zejména z hlediska existujících rizik a jejich závažnosti. Následně bude uvedeno několik případů z mé policejní praxe a rovněž několik více či méně mediálně známých, avšak typických, tuzemských i zahraničních kauz zneužití prostřednictvím sociálních sítí. Tyto případy budu následně analyzovat z hlediska rizik a možností prevence. V závěru své práce bych uvedl rady, jak nebezpečím předcházet včetně rad jak postupovat, když už k nějakému pochybení v obezřetnosti a k následné reálné hrozbě zneužití dojde.

TEORETICKÁ ČÁST

2. Výklad základních pojmů

V této části bych rád uvedl několik pojmů nevhodného či protiprávního jednání, nebezpečí a hrozeb, které mohou číhat nejen na děti, mládež, ale i na dospělé v prostředí internetu resp. v prostředí sociálních sítí.

Začal bych však nejprve obecně, a to stručným popisem základních pojmů, se kterými se bude čtenář v mé práci pravidelně setkávat.

2.1. Internet

Internet je propojení jednotlivých počítačů pomocí síťových prvků a kabelů, kdy tyto počítače mezi sebou komunikují pomocí protokolů.

Internet je pro lidstvo obrovských přínosem. Dá se říci, že lidem hodně usnadňuje práci. Dříve člověk musel složitě hledat v knihách, chodit za zkušenějšími lidmi apod. V současné době si pouze otevře internetový prohlížeč, zadá do něj klíčové slovo a už mu „vybíhá“ nepřeberné množství odkazů k zadanému slovu či tématu. Zároveň je však nutné, abychom s ním uměli zacházet, znali jeho klady, ale hlavně i jeho zápory a nebezpečí, která na něm číhají a jak těmto hrozbám předcházet, případně když už k nějakému reálnému ohrožení dojde, jak v takové situaci postupovat.

2.2. Kyberprostor aneb prostředí, ve kterém dochází k rizikovému chování

Nejprve by bylo vhodné definovat prostředí, ve kterém se níže uvedené protiprávní jednání odehrává. Ve skutečnosti totiž jednání, která budu popisovat, vychází z činností (šikana, pronásledování, krádeže apod.), které se praktikovaly již dříve, ale v posledních dvou či třech desítkách let, se jejich těžiště přesunulo do prostoru, kde člověk tráví většinu svého ať již pracovního nebo volného času. Jde o kyberprostor.

Kyberprostor jako pojem, byl poprvé použitý v roce 1982 Williamem Gibsonem v roce 1984 jako ústřední téma jedné povídky jeho románu Neuromancer. Věra Zelinková definuje kyberprostor jako nehmotný svět informací, který vzniká vzájemným propojením informačních a komunikačních systémů. Toto prostředí umožňuje vytvářet, uchovávat, využívat a vzájemně si vyměňovat informace. Zahrnuje počítače a databáze propojené komunikačními systémy jako například celosvětovou síť internet. (1)

2.3. Sociální sítě

V případě sociálních sítí jde de facto o společenskou síť, službu na internetu, která umožňuje po registraci a vytvoření osobního profilu komunikovat s ostatními registrovanými uživateli, sdílet s nimi informace, fotografie, videa a provozovat další aktivity.

Sociální sítě se dělí na osobní a profesní. Mezi v České republice nejznámější a nejpoužívanější osobní sociální sítě patří Facebook, Youtube, Lidé, Twiter. Dalšími hojně používanými jsou MySpace, Badoo, Spoluzaci, Linkuj a další. Do profesních sítí lze zařadit u nás nejpoužívanější LinkedIn, dále ve světě používané Visible.me, či Xing. Dle odhadů existuje přibližně 200 komunitně zaměřených sociálních sítí, které využívá 46% populace na celém světě.

První varianty internetových sociálních sítí vznikly v polovině 90. let minulého století a jednalo se o sítě v rámci internetových stránek Geocities (1994), Theglobe.com (1995) nebo Tripod.com (1995). Druhá a vylepšená generace sociálních sítí přišla ve druhé polovině 90. let a umožňovala si vytvořit profil a propojit se s přáteli. Jednalo se o projekt Sixdegrees.com, který fungoval v letech 1997 až 2001. Tyto sociální sítě položily základ pro fungování dnešních sociálních sítí. (2)

2.3.1. Facebook

Sociální síť Facebook založili 1. února 2004 Mark Zuckerberg a Edduard Severin původně jako systém komunikace mezi studenty Harvardské univerzity, kdy se k této síti postupně připojovaly další univerzity. Od začátku roku 2006 se k Facebooku začaly připojovat některé nadnárodní společnosti až se Facebook s počtem 1,5 miliardy uživatelů a s počtem 84 jazykových verzí vypracoval na jednu z nejpoužívanějších sociálních sítí na světě. Facebook je určen pro osoby starší 13 let a předpokladem je založení svého osobního profilu pod svým skutečným jménem. (3)

2.3.2. Lide.cz

Internetový portál Lide.cz je prostor pro poznávání nových lidí a moderní seznamovací služba provozovaná portálem Seznam.cz. Tato služba dříve nabízela velké množství chatovacích místnosti rozdělených podle žánrů jako například seznámení, koníčky, sport, avšak tato funkce byla zrušena a nahradila jí moderní internetová seznamka ve stylu sociální sítě Badoo.

2.3.3. Badoo

Je komunitní síť založená v roce 2006 ruským podnikatelem Andreyem Adreevem, která se zaměřuje na seznamování lidí po celém světě. Je přeložen do 40 jazyků včetně češtiny a čítá 311 miliónů uživatelů. Registrace a základní funkce jsou bezplatné, rozšířené služby jsou zpoplatněné. (4)

2.4. Nevhodné a protiprávní jednání na sociálních sítích

Než začnu psát o závažných, protiprávních jednáních, rád bych zmínil dvě rizika, a to spíše psychologického rázu, která však nejsou v případě zejména dětí zanedbatelná.

2.4.1. Odtržení od reality

Jak uvádí Sborník studií Děti a online rizika: Základními negativními rysy internetového prostředí je možnost nepřirozeného úniku do světa fantazie počítačových her, virtuálních lákadel a „online efekt ztráty zábran“. Útěk do fantazie pak přináší hodiny strávené na internetu, ochlazování a uvádění skutečných vztahů na úkor těch virtuálních, jednoduše – žití života více na síti než v reálu. Ztotožňuju se i s tam uvedeným názorem, že příčinou takového úniku z reality může být neúspěch ve vztazích ve skutečném životě kvůli strachu, nedostatečným komunikačním dovednostem, kvůli hendikepu či např. izolaci. (5)

Na internetu můžeme být tím, kým chceme. Můžeme si vytvořit vlastní identitu, která s realitou nebude mít nic moc společného. Napomáhá tomu i jisté odosobnění, fakt, že sedíme za počítačem a komunikujeme přes internet s lidmi, kteří sedí také za počítači, je mezi nimi určitá vzdálenost, komunikace postrádá vizuální i tělesný kontakt. Nezáleží na tom, jak vypadáme, jestli jsme obézní, s malou tělesnou výškou, s nějakým handicapem. Na internetu resp. sociálních sítích můžeme být kýmkoliv, koho si vysníme, vytvoříme. Buď si dáme na svůj profil na sociální síti fotografii někoho „dokonalého“ nebo nemusíme, stačí se tak popsat, vykreslit a „dokonalý“ život ve virtuální realitě může začít.

2.4.2. Závislost na internetu resp. sociálních sítích

Pro příklad závislosti na internetu resp. sociálních sítích nemusíme chodit až tak daleko. Stačí na to třeba cestovat městskou hromadnou dopravou a rozhlédnout se kolem sebe. Kolik lidí má v ruce mobilní telefon a s někým si dopisuje prostřednictvím nepřeberného množství aplikací jako je například messenger, viber, whatsapp apod. nebo pouze „projíždějí“ timeline

svých přátel na Facebooku. Této formě komunikace mezi lidmi v poslední době značně napomáhá i fakt, že mobilní operátoři pod tíhou konkurenčního boje učinili mobilní data dostupnějšími. Už neplatíme za drahé, vytáčené, internetové připojení, k neomezenému mobilnímu tarifu dostaneme jako bonus přibližně 1,5 GB dat, která bohatě stačí na komunikaci prostřednictvím sociálních sítí na celý měsíc.

Jednu dobu jsem byl také závislý na sociální síti. Bylo mi 22 let. Byl krásný, jarní den. Víkend. Nebe bez mráčku. Byl jsem na chatě přibližně 25 km od Prahy. Idylka? Jak pro koho. Pro člověka závislého na internetu a sociálních sítích ne. Takže jsem pospíchal domů, abych si sedl co nejdříve k počítači, přihlásil se na svůj profil na jednom malém chatu, kde jsem měl vybudovanou určitou již respektovanou pozici a mohl tak „žít“ svůj vysněný, pro mě v tu dobu ideální, virtuální život.

Podobně závislých lidí, hlavně dětí a dospívajících, jsou desetitisíce. Jen si zkuste dětem zabavit mobilní telefon nebo tablet. O následných negativních reakcích dětí jsem se přesvědčil sám na škole v přírodě jedné pražské základní školy, se kterou jsem jel jako vychovatel. Před odpolední vycházkou jsme vybrali mobilní telefony, jednak aby děti dávaly pozor na cestu a jednak aby je po cestě neztratily. Děti sice mobilní telefony dobrovolně vydaly, ale tento úkon doprovodily velice zpomalenými pohyby a nesouhlasnými komentáři. A to bylo v době, kdy se ještě nejednalo o chytré telefony s připojením na internet a s velkým množstvím nainstalovaných her. I jedna moje kolegyně z práce zkoušela, jak dlouho vydrží bez mobilního telefonu a tím pádem bez přístupu na sociální síť. Pro jistotu mobilní telefon rozebrala na jednotlivé součástky, vyndala ven baterii a všechny díly zamkla do šuplíku. Klíč předala kolegovi z vedlejší kanceláře. Vydržela to asi 2 hodiny a následně šla prosit kolegu, aby jí klíč vydal.

O tom, že závislost na internetu je rozšířený, globální problém, svědčí i případ z Číny, kde však tuto závislost řešili velice svérázným a nelidským způsobem. Studie z roku 2009 odhalila 24 miliónů lidí ve věku 13-29 let digitálně závislých. Dokonce tam byly vytvořeny tábory pro takto závislé osoby na internetu, kde byl do těl závislých pouštěn elektrický proud. (6) O humánnějších metodách, jak odvést dětem pozornost od internetu, bych se rád zmínil v metodické části mé práce.

A teď již k samotným nevhodným či protiprávním jednáním. Jak jsem již psal výše, jedná se o nevhodné či protiprávní jednání, které člověk zažíval již dávno, jako například šikanu

či stalking, kdy s rozvojem počítačových, mobilních a internetových technologií se toto jednání přesunulo do již zmíněného kyberprostoru a vznikla tak kyberšikana a kyberstalking.

2.4.3. Kyberšikana

Kyberšikana, která je v anglické literatuře označována jako Cyberbullying, nemá jednotnou definici. Dle knihy Bullying Beyond the Schoolyard se jedná o úmyslné a opakované ubližování způsobované prostřednictvím používání počítačů, mobilních telefonů a dalších elektronických zařízení. (7)

Jde vlastně o podobnou šikanu, která je páchána třeba na školách nebo byla páchána na vojně, avšak tato šikana probíhá pomocí počítačů a mobilních telefonů, prostřednictvím zasílaných zpráv přes internet či sms zpráv, apod.

Dalším znakem kyberšikany je fakt, že ve většině případů se oběť a útočník znají i v reálném světě například ze školy nebo z práce, a to již delší dobu, díky čemuž útočník ví, co na oběť platí a tyto informace v šikaně v kyberprostoru zneužívá.

Na rozdíl od následujících dvou pojmů se nemusí vyloženě jednat o protiprávní jednání, každopádně jde o nevhodné chování, které se může řešit a zdárně vyřešit především na úrovni školy, prostřednictvím učitelů, výchovného poradce nebo rodičů bez účasti policie či jiných orgánů státní správy.

2.4.4. Kybergrooming

Pojem Kybergrooming vychází z anglického slova grooming, kdy sborník studií Děti a online rizika rozlišuje pojem allogrooming, což ve zvířecím světě označuje proces starání se či pečování jednoho člena skupiny o druhého a pojem grooming v lidském světě jako synonymum milostného poměru, důvěry, rodičovské lásky a péče. (5)

Kybergrooming není na internetu ani v literatuře jednoznačně definován. Dá se říci, že jde o nevhodné chování uživatelů moderních komunikačních technologií často spočívající ve vydávání se za jinou osobu (vrstevníka oběti), což internetová anonymita snadno umožňuje (získání důvěry oběti s cílem od oběti vylákat pornografický materiál nebo oběť vylákat na osobní schůzku a zpravidla jí sexuálně zneužít). V omezených případech může jít i o majetkovou trestnou činnost, kterou blíže rozvedu v podkapitole majetková trestná činnost a zároveň uvedu několik konkrétních příkladů z mé praxe a jeden mediálně známý případ.

Na rozdíl od kyberšikany je cíl útočníka a i samotný průběh jiný. Nejde o to oběť šikanovat, ponížit či zesměšnit, ale nejdříve svojí oběť upoutat, vybudovat vztah (povídáním například o hrách, zvířátkách, kupováním dárečků, kreditu, apod.), vzbudit důvěru, často oběť psychicky izolovat od rodiny, kamarádů a poté, co se mu to podaří, oběť přesvědčit k zaslání erotických fotografií či k osobní schůzce a následně ji sexuálně zneužít. Z tohoto plyne fakt, že se většinou útočník s obětí ze začátku nezná a vybírá si ji náhodou. O to obtížnější může být následné vypátrání útočníka, protože s obětí ho spojuje jen vzájemná elektronická komunikace a většinou žádné jiné osobní vazby.

Oběti groomerů jsou ve většině případů dívky ve věku 11-17 let z různých socioekonomických poměrů. Snazší oběti jsou z řad ekonomicky slabších a z okruhu méně vzdělaných lidí. Nejmladší děti nejsou groomery tolik ohroženy, jelikož nejsou ještě tolik aktivní v kyberprostoru.

O tom, že kybergrooming je reálná a všudypřítomná hrozba, se přesvědčilo několik novinářů a kriminalistů, kteří založili fiktivní profily nezletilých dívek, kdy během pár hodin je kontaktovalo několik osob s žádostí o jejich nahé fotografie.

Následky kybergroomingu mohou být relativně neškodné, kdy mezi groomerem a jeho obětí může probíhat pouze elektronická komunikace, avšak může mít i fatální následky, kdy se groomerovi může podařit oběť vylákat a zneužít a v krajním případě i zavraždit.

2.4.5. Kyberstalking

Při sledování zábavných videí na internetovém portálu youtube.com, mě zaujalo jedno video, které bylo natočeno pro belgickou federaci finančního sektoru Febelfin s internetovými stránkami safeinternetbanking.be, ale ze začátku tomu vůbec nic nenasvědčovalo. Hlavní postavou tohoto reklamního šotu je Dave, mimořádně nadaný jasnovidec. Ten si zve do svého bílého stanu náhodně vybrané lidi z ulice a postupně odkrývá jejich soukromí, kdy hádá, kdo je jejich kamarád/kamarádka, jaké mají vozidlo či motocykl, co zrovna v současné době prodávají a nakonec uhádne i jejich číslo účtu a výši a artikl jedné z jejich posledních bankovních transakcí. Ve skutečnosti Dave není žádný jasnovidec ani mentalista, ale pouze herec, který si na jasnovidce pouze hraje a dostává informace od skupiny IT specialistů, kteří sedí hned ve vedlejší části stanu u počítačů a na internetu vyhledávají všechny dostupné informace, které získali z drobných střípků konverzací Davea s do stanu pozvanými osobami. I když se jedná reklamní o materiál belgického sdružení Febefin, které chce upozornit hlavně na využívání

bezpečného bankovnictví, krásně nám ukazuje, jakou elektronickou nebo-li digitální stopu za sebou lidé nechávají a co všechno se dá z jimi poskytnutých údajů zjistit a následně nejen stalkerem zneužít.

Kyberstalking vychází z pojmu stalking (tento výraz se do českého jazyka nepřekládá), což je nevhodné, často protiprávní jednání, které se projevuje opakovaným fyzickým sledováním určité osoby, sbíráním informací o ní apod. Na rozdíl od klasického stalkingu, se kyberstalking, tedy v doslovném předkladu pronásledování v kyberprostoru, odehrává, jak již název napovídá, v prostředí internetu, prostřednictvím emailové komunikace, komunikace na sociálních sítích, prostřednictvím mobilních telefonů apod. Stalker, jak se nazývá osoba, která svojí oběť pronásleduje, je většinou zhrzený milenec/milenka, nesnášenlivý kamarád/kamarádka, platonicky zamilovaný jedinec, tedy osoba, která svojí oběť většinou zná i v reálném životě. V ojedinělých případech se může jednat i o náhodné vybrání své oběti na internetu či pronásledování nějaké celebrity, tedy lidí, se kterými se stalker osobně nikdy nesetkal.

Velký nárůst stalkingu je přičítán právě rozvoji internetových technologií a praktikování právě kyberstalkingu. Stalking je trestným činem v USA již od roku 1990, v České republice byl do právních předpisů resp. do trestního zákoníku stalking zakotven až v roce 2010, a to pod pojmem nebezpečné pronásledování dle § 354 zák. č. 40/2009 Sb. trestního zákoníku.

Problém je však často v určení, zda pronásledování naplňuje skutkovou podstatu trestného činu nebezpečného pronásledování či nikoliv. Chování či jednání pachatele totiž může zprvu naplňovat pouze skutkovou podstatu přestupku, jelikož útočník v případě stalkingu nejdříve zasílá oběti urážlivé sms zprávy, emaily, či zprávy přes sociální sítě. Teprve následně může své jednání stupňovat v poškozování a ničení věcí oběti a vše může vyvrcholit zraněním či smrtí oběti.

2.4.6. Sexting

Když si otevřeme bulvární stránky na internetu, brzo na nich narazíme na nějakou známou osobnost, v drtivé většině ženského pohlaví, která je více či méně odhalená. Je známo, že tyto známé osobnosti jsou často vzory hlavně pro dospívající, kteří se je snaží napodobovat. Když pak tyto své vzory vidí, jak se bez bázně a hany odhalují, získají dojem, že je to běžná věc, že díky tomu člověk může získat obdiv okolí, přízeň někoho, kdo se jim líbí a také se

odhalují či posílají své erotické fotografie ať už známým nebo neznámým lidem přes internet. A v té chvíli nastává nebezpečí zneužití těchto explicitních materiálů.

Pojem sexting vznikl spojením slov „sex“ a „texting“. Jde o zasílání textů, fotografií a videí s erotickým a sexuálním obsahem prostřednictvím elektronických médií jako jsou sms zprávy, emaily, mms, zprávy přes sociální sítě apod. Zasílání takovéhoto materiálu je dobrovolné, oběti sextingu si neuvědomují, že erotický materiál je náchylný k následnému zneužití, vydírání, ale i pouze jako předmět k veřejnému zesměšnění. Nezletilé děti si taktéž neuvědomují fakt, že zasíláním byť vlastních intimních fotografií, mohou samy tímto činem spáchat trestný čin, a to výrobou a šířením dětské pornografie.

Sexting provozují nejčastěji děti starší 15 let, které své erotické fotografie zasílají svým vrstevníkům. Výjimkou nejsou ani dospělí jedinci, kteří zasílají fotografie své nahé postavy nebo jen jejich částí cizím lidem, se kterými se seznámili na chatech nebo internetových seznamkách.

2.4.7. Majetková trestná činnost v kybeprostoru

Krádeže či pokusy o ně jsou staré, jako lidstvo samo. Formy a různé techniky zlodějů a lapků se vyvíjely s vývojem lidstva a s tím, jak lidé svůj majetek chránili. Když lidé začali své peníze chránit před odcizením v trezorech, začali pachatelé vymýšlet, jak se do těchto zabezpečených schránek dostat. V době mohutného rozvoje výpočetní techniky se většina finančních transakcí změnila z hotovostních na bezhotovostní. I když stále platíme v obchodech penězi, čím dál více začínáme využívat platební karty a bezhotovostní platby převody na účet. V dnešní době prakticky nedostanete výplatu v hotovosti, ale musíte mít založený bankovní účet. V poslední době nastal obrovský rozmach internetových obchodů, kterým ty kamenné obchody mohou v některých ohledech jen těžko konkurovat. Těmto novým trendům se přizpůsobují i pachatelé majetkové trestné činnosti, kteří přicházejí s často rafinovanými způsoby, jak se k této nové formě uchovávání a nakládání s penězi dostat. A proto využívají činnosti jako skimming, což je kopírování platebních karet pomocí speciálního čtecího zařízení, které pachatelé umísťují do bankomatů či v ojedinělých případech načítají data pomocí zařízení, kdy jim stačí pouze krátká vzdálenost mezi kartou a takovým zařízením.

Mezi další sofistikovanou dovednost, kterou pachatelé ovládají a využívají, je phishing, někdy překládaný do češtiny jako rhybaření, což je činnost používaná na internetu k získávání citlivých dat jako jsou hesla k bankovním účtům, čísla a hesla kreditních karet apod. Vylákání

těchto citlivých informací bohužel napomáhají i sociální sítě a chaty, pomocí kterých se pachatelé s oběťmi spojují, komunikují a následně získaná data a informace zneužijí.

Další možností pachatelů, jak se snadno a relativně rychle dostat k penězům, je vkládání podvodných inzerátů na internet. Podvodníci často volí taktiku známou z hodin marketingu a managementu, kdy méně znamená více, a tak dávají inzeráty se zbožím za nižší ceny, kdy se na toto „nachytá“ větší množství lidí a pachatel tak v konečném zúčtování získá větší objem finančních prostředků, čítajících často i statisíce. V poslední době však nízké ceny začaly být kupujícím podezřelé, proto začali kriminálníci nastavovat jen o něco málo výhodnější ceny než na trhu zajeté internetové obchody. Pro větší důvěryhodnost podvodníci již nezakládali své emailové účty u freemailových poskytovatelů (např. seznam.cz, centrum.cz apod.), ale zakládali si vlastní domény s vlastními podvodnými internetovými stránkami a firemními emaily. Než došlo k zablokování těchto stránek poskytovatelem služeb na žádost policie, spadlo do sítě podvodníků několik desítek až stovek poškozených. Je mi znám jeden případ podvodníka, který si založil jeden internetový obchod, kdy trval na platbách předem a zboží nikdy nezasílal. Když se po nějaké době zjistilo, že vše slouží jen k páchání kriminální činnosti, obchod sám zrušil a založil si nový. Toto činil pořád dokola a své „podnikání“ řídil ze zemí, které neměly s Českou republikou smlouvu o vydávání podezřelých. Často to bylo z lehátka někde u moře.

Na vzrůstající oblibu sociálních sítí zareagovali pachatelé spíše drobnějších majetkových trestných činností, kteří z uživatelů sociálních sítí lákají menší částky do 5000 Kč, a to z více důvodů. Jednak z toho důvodu, že se jedná o provinění v přestupkové rovině, kdy spáchání takovýchto činů není trestným činem a postih za takovéto jednání je menší a jednak proto, že v takovém případě jsou i oprávnění policie, co se týče následného šetření po pachatelích, omezená. Tato situace se mění v případě, kdy pachatelé často v protiprávních činnostech pokračují a souhrnná škoda tak přesáhne hranici oněch 5000 Kč. Pravděpodobnost odhalení útočníků se tím pádem diametrálně zvyšuje a i následný trest je přísnější.

PRAKTICKÁ ČÁST

3. Rozbor zahraničního a tuzemského výzkumu

Po konzultaci s pracovníky Národního centra bezpečnějšího internetu, jsem si k rozboru vybral jeden tuzemský výzkum, a to Výzkum rizikového chování českých dětí v prostředí internetu 2014 a soubor zahraničních výzkumů v rámci projektu EU KIDS ONLINE 2014.

Oba uvedené výzkumy jsou ve většině aspektů těžko srovnatelné, jelikož poskytují minimum výstupních dat, která by byla vzájemně porovnatelná. Dále jsou v obou výzkumech značné rozdíly v procentuálních hodnotách ve srovnatelných bodech, jejichž rozklíčování by byl úkol spíše pro sociologa. Z výše uvedených důvodů bych se proto věnoval spíše rozboru obou výzkumů, a to z pohledu preventisty (policisty/vychovatele) rizikového chování a na základě výsledků průzkumů vytipoval oblasti, na které je třeba se primárně zaměřit a ze kterých vyplývají, byť ne co do četnosti, ale co do nebezpečnosti, největší potenciální rizika pro děti a mládež.

Nejdříve bych popsal to, co mají oba výzkumy společné a v čem se liší, poté bych uvedl stěžejní otázky, odpovědi a názory na rizika v prostředí internetu z pohledu dětí v jednotlivých výzkumech. Na závěr bych provedl analýzu vybraných bodů a zjištění z obou průzkumů, které považuji za klíčová. Zaměřil bych se zejména na vyhodnocení silně alarmujících výsledků, které přímo volají po osvětě v této problematice, ke které by měla napomoci i tato bakalářská práce.

3.1. Co mají oba výzkumy společného?

Oba výzkumy byly provedeny kvantitativně formou dotazníku. V případě českého výzkumu byla získána zpětná vazba od 28232 dětí, kdy tomuto předcházelo zaslání emailů se 71 otázkami do 4200 škol a 40000 vzkazů přes sociální sítě. Evropský výzkum obsahoval zpětnou vazbu od srovnatelného množství respondentů, a to od 25000 osob včetně rodičů dětí. Výsledky obou průzkumů byly po nashromáždění a zanalyzování dat zveřejněny v roce 2014.

3.2. Rozdíly v obou výzkumech.

Český výzkum byl zaměřen na aktuální situaci dětí v prostředí internetu v roce 2014. Evropský výzkum na rozdíl od českého byl spíše zaměřen na porovnání aktuálního stavu v roce 2014 s vybranými výsledky předchozího evropského výzkumu, který proběhl v rámci stejného projektu v letech 2009-2011.

Rozdíl v obou průzkumech je i co se týče věkového rozpětí dotazovaných dětí, kdy v případě českého výzkumu byly dotazovány děti ve věku 11 až 14 let a děti ve věku 15 až 17 let, zatímco v případě evropského výzkumu byly některé otázky (omezené vzhledem k nízkému věku dotazovaných) pokládány i skupině dětí ve věku 9 a 10 let. Ostatní dvě skupiny dětí byly věkově srovnatelné s českým výzkumem, kdy jedna skupina byla ve věku 11 až 13 let a druhá 14 až 16.

Další důvod prakticky znemožňující srovnání je rozdílnost ve stylizaci otázek v jednotlivých výzkumech. Z tohoto důvodu provedu rozbor jednotlivých výzkumů.

3.3. Evropský výzkum EU KIDS ONLINE

Aktuální zahraniční výzkum s názvem EU Kids online probíhal v letech 2011-2014 pod vedením profesorky Sonia Livingstone, LSE a byl financován Evropskou komisí z programu Safer internet.

Projekt srovnává zjištěná aktuální data s výsledky předchozího výzkumu, který proběhl v letech 2009-2011 v 25 evropských zemích a oslovil 25000 dětí a rodičů. V tomto projektu se počet zúčastněných zemí zvýšil na 33 a rozšířil se i okruh kladených otázek.

3.3.1. Co dělají děti na internetu?

Projekt EU Kids online 2010 poskytl data z 25 zemí.

Sesterský projekt Net Children Go Mobile z roku 2014 provedl aktualizaci dat, kdy se jednalo o výstup ze 7 evropských zemí, a to Belgie, Dánsko, Itálie, Irsko, Portugalsko, Rumunsko a Velká Británie.

Z výsledků průzkumů z let 2014 a 2010 je patrné, že ve všech uvedených bodech, co se týče aktivit na internetu či používání výpočetní techniky, došlo k menšímu či většímu nárůstu. K jednomu z největších rozdílů došlo v případě navštěvování sociálních sítí dětmi, a to ze 44 % v roce 2010 na 63%. Tento fakt je, jak jsem již uvedl, spojen s větší dostupností výpočetní techniky a se vzrůstající technickou gramotností dětí. K dalšímu relativně velkému rozdílu došlo v případě sdílení blíže nespecifikovaných fotek, videí a hudby dětmi s ostatními dětmi, a to z 6% v roce 2010 na 20% v roce 2014. K ještě většímu rozmachu došlo na poli sledování videí dětmi (např. na youtube apod.), kdy tuto činnost provozovalo v roce 2010 32 % dětí a v roce 2014 necelých 60 % dětí (59 %). V dalších bodech již takové rozdíly nebyly.

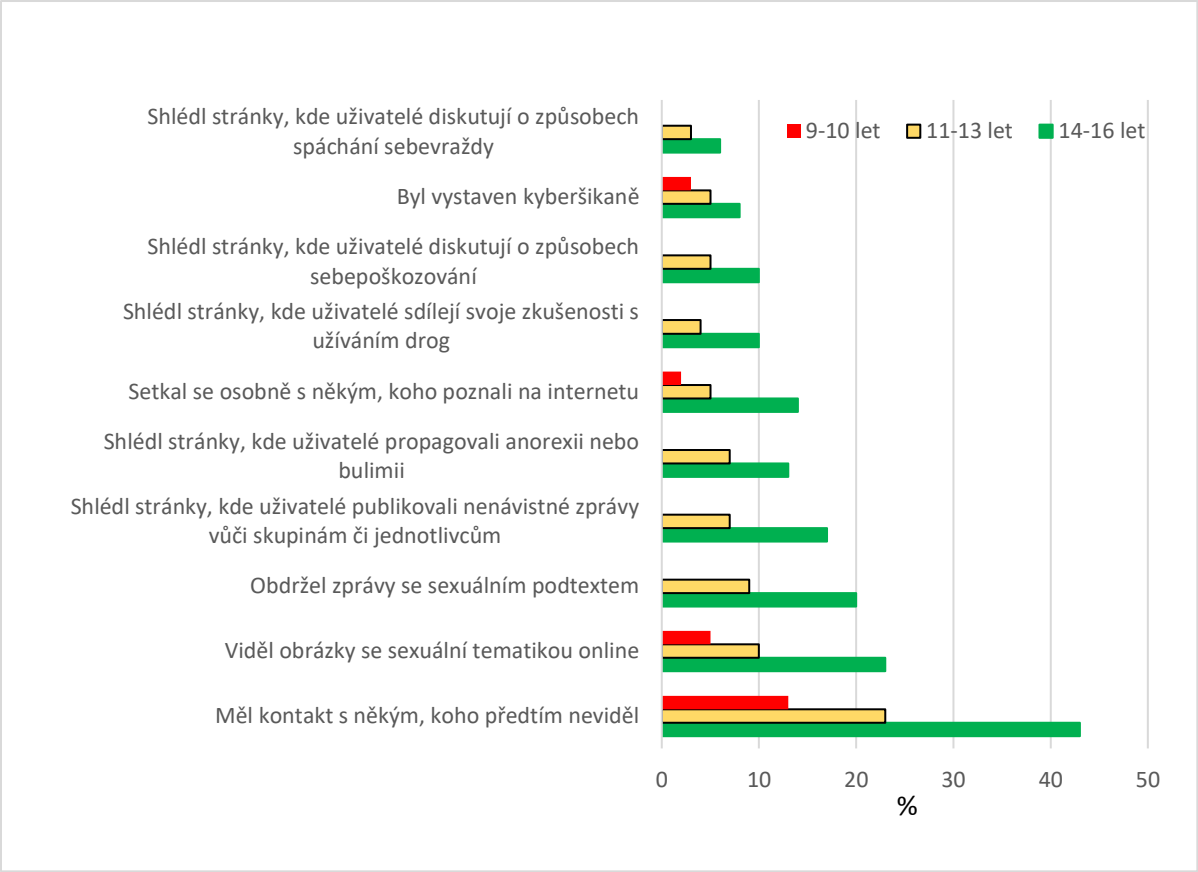
3.3.2. Co děti znepokojovalo?

Téměř 10 tisíc dětí bylo dále osloveno, aby vlastními slovy popsaly, co obtěžuje, nebo znepokojuje děti jejich věku na internetu. Věk dětí se pohyboval v rozmezí 9-15 let. Bylo zjištěno pět klíčových skutečností:

- děti nejvíce na internetu znepokojuje přítomnost pornografie.
- v těsném závěsu za prvním bodem děti znepokojuje zobrazování násilí, obzvlášť reálné násilí na bezbranných (děti, zvířata)
- jako nejčastější zdroj násilných, pornografických a jiných znepokojujících rizik děti vnímají stránky na sdílení videí
- chlapci vyjadřují největší obavy z násilí, dívky mají největší strach z kontaktování cizí osobou
- zatímco mladší děti jsou více znepokojeny rizikovým obsahem, starší děti jsou více znepokojeny riziky spojenými s kontaktem s neznámou osobou

3.3.3. S jakými online riziky se děti setkaly?

V projektu EU Kids Online 2010 byly srovnány konkrétní věkové skupiny, a to 9-10 let, 11-13 a 14-16. Otázky se týkaly online rizik, s jakými se děti setkaly na internetu. Věkové skupině 9-10 let nebyly z etických důvodů pokládány některé otázky. Výsledky jsou shrnuty v Obr. 1.



Obr. 1: Srovnání rizik, se kterými se děti setkaly v roce 2010 podle věkových skupin. Zdroj: Závěrečná zpráva EU KIDS ONLINE 2014.

Čtyři základní zjištění průzkumu věkových skupin 11-13 let a 14-16 let co se týče online rizik:

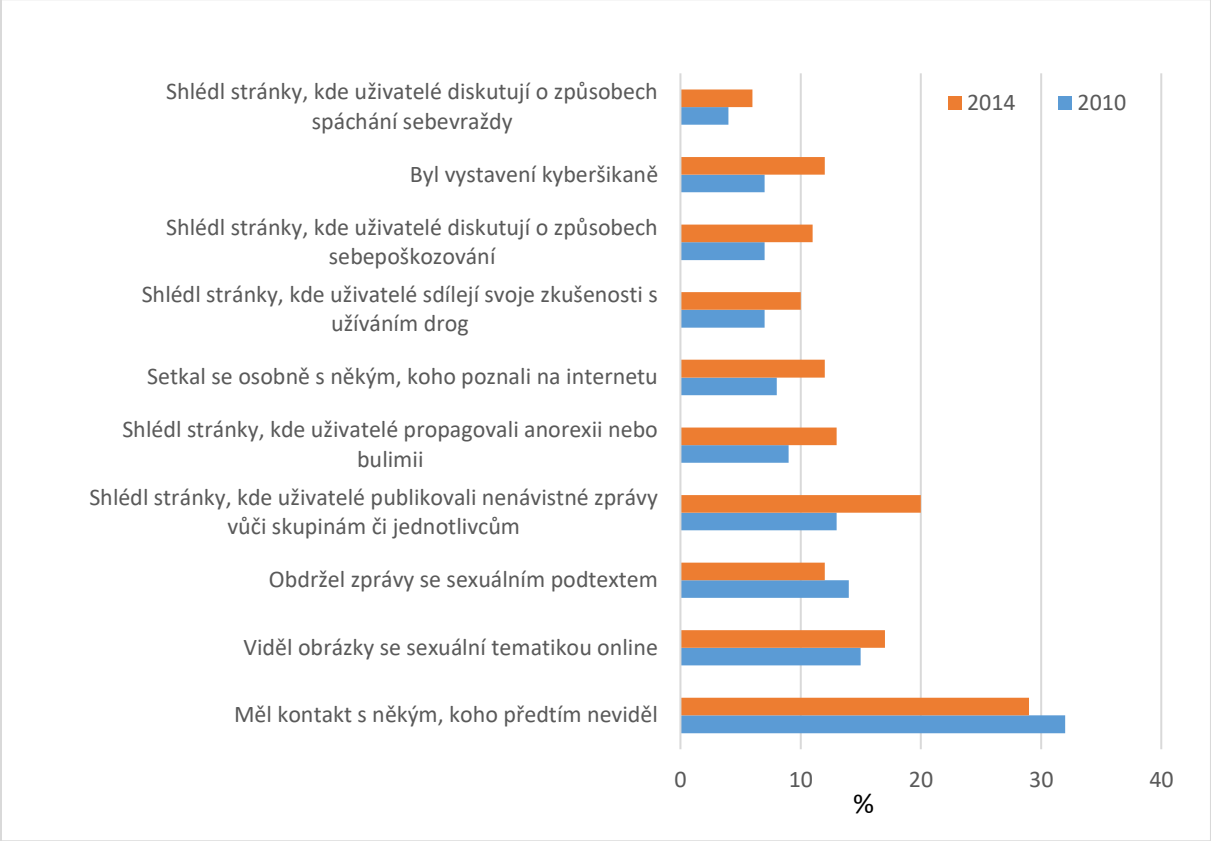
1) nejčastější riziko je kontaktování dítěte někým, koho dítě osobně nezná

2) další nejčastější riziko je shlédnutí obrázků a obdržení zpráv se sexuální tématikou; vystavení pornografii bylo více hlášeno chlapci a staršími dětmi a někteří (ale ne všichni) toto shledali nevhodným; při srovnání napříč zeměmi vystavení sexuálním rizikům bylo více typické pro země, kde rodiče nechávají dětem více prostoru a svobody

3) nevhodný obsah, který vkládají a šíří sami uživatelé; u těchto rizik se očekává vzestup společně s tím, jak se do vytváření zapojují více dětí; tato rizika dostávají málo pozornosti od kompetentních osob, které vytvářejí uživatelské zásady, a to i z toho důvodu, že kromě blokování stránek je těžké vyvinout nástroje, které odfiltrují nevhodný obsah; do rizikového obsahu patří i nenávistný, pro-anorektický obsah, stránky, kde dochází k diskuzím ohledně užívání drog, sebepoškozování apod.

4) kyberšikana, která je hlášena poměrně malou skupinou 11-16 letých, nicméně toto riziko má největší pravděpodobnost ke způsobení újmy dítěti; polovina těchto dětí hlásila, že byla velmi znepokojena obdržením nepříjemných či zraňujících online zpráv.

Data z roku 2010 byla aktualizována v sedmi zemích v roce 2014, viz Obr. 2.



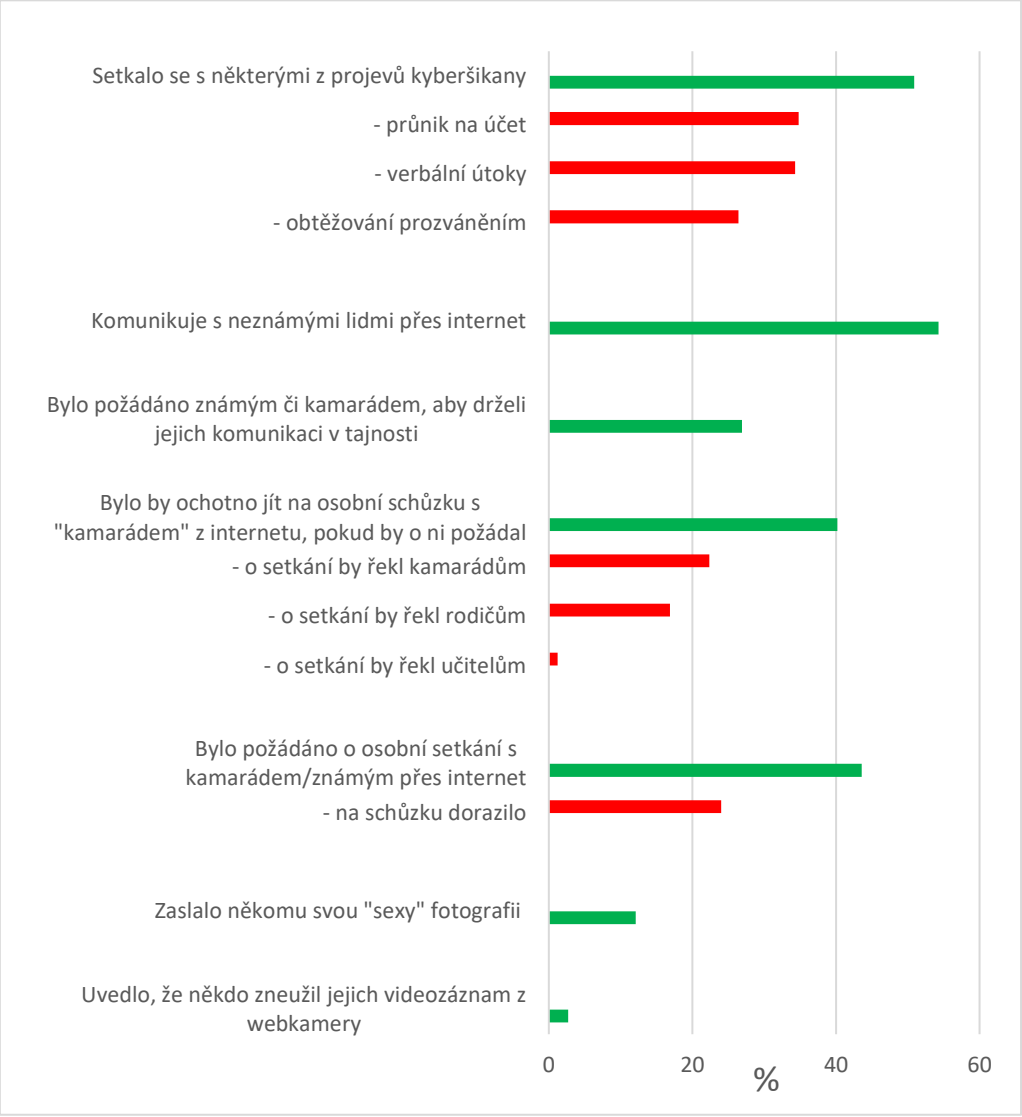
Obr. 2: Srovnání rizik, se kterými se děti setkaly v letech 2010 a 2014. Zdroj: Závěrečná zpráva EU KIDS ONLINE 2014.

Z výše uvedeného srovnání vyplývá, že děti jsou nyní (2014) více vystaveny nenávistným zprávám, pro-anorektickým a sebepoškozovacím stránkám a dále kyberšikaně. Naproti tomu děti jsou opatrnější co se týče online kontaktů od neznámých osob. Autoři připouštějí jistou účinnost snah o upozorňování na toto nebezpečí. Nicméně děti se s větší pravděpodobností nechají vylákat cizí osobou ke kontaktu v reálu.

3.4. Výzkum rizikového chování českých dětí v prostředí internetu 2014

Poslední rozsáhlý výzkum chování českých dětí v prostředí internetu je z roku 2014 a proběhl pod vedením Mgr. Kamila Kopeckého, Ph.D., z Univerzity Palackého v Olomouci. Jak jsem již uvedl výše, v rámci výzkumu bylo rozesláno 71 otázek formou emailu do 4200 českých škol a formou 40000 vzkazů přes sociální sítě, kdy zpětnou vazbu poskytlo 28232 dětí ve věku

od 11 do 17 let. Cílem výzkumu bylo převážně zjistit, zda a jaké mají děti zkušenosti s pojmy jako je kyberšikana, kybergrooming, sexting, používání webkamery, sdílení a zasílání osobních údajů a s používáním sociálních sítí. Vybrané výsledky jsou graficky vyjádřeny v Obr. 3.



Obr. 3: Rizika, se kterými se setkaly děti v ČR a jejich případné reakce v těchto situacích. Zdroj: Výzkum rizikového chování českých dětí v prostředí internetu 2014, UPOL.

Český výzkum oproti evropskému výzkumu šel doplňujícími otázkami více do hloubky problému. Například v případě kyberšikany rozebírá čeho konkrétně se kyberšikana týká: verbálních útoků, obtěžování prozváněním, ponižování, krádežemi identity apod. Dále postihuje například i tu oblast zkoumání, kolik procent dětí, by se s jakými projevy kyberšikany svěřilo rodičům a kolik učitelům. Podrobnější je i v tom, jaké konkrétní informace o sobě děti na internetu sdělují.

Konkrétní výsledky vybraných bodů českého výzkumu budu podrobněji rozebírat v následující kapitole.

3.5. Rozbor nejdůležitějších bodů a zjištění

V prvních dvou podkapitolách jsem uvedl chování a rizika na internetu z pohledu dětí. V této podkapitole bych však úhel pohledu obrátil a zaměřil se na rizika z pohledu preventisty.

Problém spatřuji právě v úhlu pohledu, kdy si děti často neuvědomují hrozící nebezpečí a je pro ně daleko znepokojující nějaká negativní zkušenost, která se jich přímo týká jako například již zmíněná kyberšikana ze strany spolužáků než fakt, že na schůzku s cizím člověkem, se kterou některé děti souhlasily a na kterou část z nich opravdu dorazila, může přijít potenciální násilník. Tomuto faktu a hazardu ze strany dětí napomáhá i to, že valná většina schůzek dětí s cizí osobou neskončila špatnou či dokonce tragickou událostí, což neznamená, že další setkání nemůže dopadnout tragicky.

Vybral jsem proto několik velice podceňovaných, ale klíčových bodů, na které by se měli preventisté, učitelé, vychovatelé a rodiče zaměřit, a to jsou:

1) *Podceňování rizik na základě malého množství osobních či zprostředkovaných negativních zkušeností*

Dle EU průzkumu jen 1 % dětí, které vyrazilo na schůzku s cizí osobou, kterou poznalo přes internet, tuto schůzku považovalo za obtěžující. Jelikož evropský průzkum nebyl tak podrobný, nebylo již zjištěno, co konkrétně se dětem na schůzce přihodilo, že ji považovaly za obtěžující.

Podobně malé procento, a to 2,67 % dětí dle českého výzkumu mělo špatnou zkušenost se zneužitím videozáznamu z webkamery, prostřednictvím které děti spolu s někým komunikovaly. Když vezmeme v potaz počet dětí, které při komunikaci přes internet používají webkameru, bude reálný počet takto „postižených“ dětí opravdu zanedbatelný.

Z výše uvedených čísel by se mohlo zdát, že je málo pravděpodobné, že se dítěti stane něco vážného, že „pouze“ uvidí na internetu sexuální či násilný obsah, maximálně si je bude někdo přes internet „dobírat“, a když půjdou s někým cizím na schůzku, tak mají téměř stoprocentní pravděpodobnost, že zažijí příjemnou zábavu a že se jim nestane nic špatného. Ale už málokdo dokáže říci či zaručit, že zrovna to další dítě nebude tím 1%, které nebude mít to štěstí a zrovna ono nezažije nějaký traumatizující zážitek či se zrovna ono nestane obětí nějakého zvrhlíka. Na pozdější výčitky pak už je většinou pozdě.

Další velice potenciálně nebezpečnou a podceňovanou záležitostí ze strany dětí je fakt, že o plánech svého jednání většinou nezpraví nikoho z řad dospělých. Dle výše uvedeného

českého výzkumu pouze 42 % dětí by o této schůzce povědělo rodičům. O něco více dětí (55,6 %) by o svém úmyslu se sejít s cizí osobou z internetu informovalo své kamarády. Jelikož se ve většině případů jedná taktéž o vrstevníky, tedy často o nezletilé osoby, nelze očekávat, že by zrovna ony mohly zabránit případnému protiprávnímu jednání.

Nízká procentuální čísla potvrzují i internetové stránky e-bezpeci.cz, které uvádějí, že jen 25% dětí by oznámilo dospělým (rodičům, učitelům, apod.) snahy kybergroomera o navázání sexuálního kontaktu.

2) *Přidávání cizích osob, které děti a mládež nikdy předtím naživo neviděly*

V EU výzkumu 29 % dětí ve věku 9-16 let komunikovalo přes internet s cizím člověkem, kterého dříve nikdy nevidělo. Dle výzkumu v ČR je to dokonce až 54,3 % dětí ve věku 11-16 let.

S výše uvedeným je spojeno následující chování, a to poskytování osobních údajů dětí neznámým lidem, kteří je kontaktovali na internetu či sociální síti. Až 62,9 % českých dětí by cizímu člověku poslalo svoje jméno a příjmení a nezanedbatelných 39 % dětí by témuž člověku zaslalo fotografii svého obličeje. Srovnatelných 38 % dětí by neznámé osobě zaslalo své telefonní číslo.

Další rizika vyplývající z obou výzkumů:

3) *Schůzka dětí s osobami, se kterými se nikdy předtím neviděly a seznámily se s nimi na sociální síti.*

Dle evropského výzkumu se 12 % dětí sešlo s osobou, se kterou se seznámilo při komunikaci na internetu. Výsledky českého výzkumu jsou opět téměř dvojnásobné, a to 24 %.

4) *Neznalost či dokonce nezájem rodičů o činnostech dětí na internetu resp. sociálních sítích.*

Zajímavá čísla a zjištění odhalil evropský výzkum z roku 2010. Například 41 % rodičů dětí, které viděly obrázky se sexuální tématikou si myslí, že jejich děti nic takového neviděly. 52 % rodičů dětí, které obdržely vulgární nebo zraňující zprávy prostřednictvím internetu resp. sociálních sítí, tuto skutečnost negovalo a dokonce 61 % rodičů, jejichž děti se setkaly s neznámým člověkem, se kterým se seznámily na internetu, o tomto setkání vůbec nevědělo.

Shrnutí nejdůležitějších bodů vyplývajících z výše uvedeného:

Rady pro děti:

- Nepodceňovat rizika na sociálních sítích
- Informovat dospělou osobu (rodiče, učitele) o svých plánech, co se týče podezřelých aktivit na internetu či schůzek s cizí osobou z internetu
- Neposkytovat cizím osobám z internetu svoje osobní údaje (příjmení, tel.čísla, adresu..)

Rady pro rodiče:

- Mít větší přehled o aktivitách dětí na sociálních sítích a obecně na internetu
- Více děti informovat o možných rizicích

4. Reálné kriminální případy

V této kapitole se budu věnovat popisu a analýze vybraných skutečných tuzemských i zahraničních případů. Nejdříve bych popsal několik případů ze své praxe. Nejedná se sice o zvlášť závažnou trestnou činnost, avšak mé případy mají určité společné rysy srovnatelné s rysy tragických příběhů, které zmíním v závěru kapitoly.

4.1. Reálné případy z vlastní praxe

U policie pracuji od roku 2009, kdy jsem, také díky mé praxi u Městského soudu, prakticky okamžitě začal pracovat na místním oddělení jako zpracovatel. Ze začátku jsem dostával ke zpracování „drobnější“ případy, a to přestupky proti majetku se škodou do 5 tis. Kč. Později jsem začal dostávat složitější případy, jako jsou provinění proti občanskému soužití, fyzická napadení (včetně napadení mezi školáky), podvodná jednání na internetu, šetření domácích násilí apod.

Pro potřeby této práce jsem vybral případy, které splňovaly kritérium poškození oběti prostřednictvím sociálních sítí.

4.1.1. Podvodné vylákání finančních prostředků prostřednictvím nabourání se do facebookového profilu

Přibližně koncem roku 2012 jsem řešil první případ podvodného jednání prostřednictvím sociální sítě, kdy nezletilá osoba oznámila, že ji přes sociální síť Facebook kontaktoval jeden její kamarád, kterého měla na Facebooku ve svém seznamu přátel s prosbou, aby mu zaslala svoje telefonní číslo, že ho omylem smazal. Dále ji požádal o to, aby mu přeposlala kód, který jí následně na toto telefonní číslo přijde. Ujistil ji, že ji to nebude nic stát. Nic netušící nezletilé během chvíle přišel na její mobilní telefon neurčitý kód, ze kterého nebylo zprvu nic poznat. Tento kód zaslala „svému“ kamarádovi prostřednictvím facebookové zprávy. Po měsíci přišla matce dívky, která za ní útratu za mobilní služby platila, faktura na několik tisíc korun. Jelikož bylo zřejmé, že pouze prostřednictvím hovorů a psaním textových zpráv nebylo možné se na takovou částku dostat, začala matka i dcera pátrat, jak k odečtení takové vysoké částky mohlo dojít. Nápovědou jim bylo podrobné vyúčtování, ve kterém byla položka jedné sázkové internetové společnosti. Jelikož nezletilá nesázela a datum odečtení odpovídal datu, kdy mladistvá komunikovala se svým kamarádem přes Facebook, bylo jí jasné, že k odečtení došlo po zaslání zmíněného kódu. Proto kontaktovala zmíněného kamaráda, který

však tvrdil, že o ničem neví. Jelikož zde však bylo podezření, které stačí na oznámení celé věci příslušnému správnímu orgánu k rozhodnutí ve věci, byla celá věc tomuto orgánu zaslána.

Případy se však začaly množit, a tento fakt společně s naprosto shodným *modus operandi* začaly nasvědčovat tomu, že se jedná o protiprávní jednání jedné osoby nebo malého počtu osob pravděpodobně navzájem spolupracujících.

Na základě šetření více podobných skutků se zjistilo, že průběh byl vždy stejný. Do náhodně vybraných, volně přístupných chatovacích místností vstupoval zaregistrovaný uživatel chatu s prosbou o hlasování pro kamarádku v nějaké modelingové soutěži. K prosbě osoba připojila odkaz na stránky, kde k hlasování mělo docházet. Na těchto stránkách se nacházely dvě prázdné kolonky pro vyplnění přihlašovacího jména a hesla na sociální síť Facebook. Po vyplnění jména a hesla se na stránce objevil nápis: Hlasování již skončilo, děkujeme za projevený zájem. Pachatel, který takto oslovoval náhodně vybrané osoby, byl zároveň administrátorem této stránky a díky tomu získal přístupové údaje na facebookové profily všech osob, které tyto své údaje v dobré víře na stránce vyplnily. Následně se na tyto profily přihlásil a oslovoval osoby, které měl ten daný profil v seznamu přátel s prosbou o přeposlání kódu, který jim přijde na jejich mobilní telefon. I když se většinou jednalo o nižší částky, většinou kolem 1500 Kč, díky oslovení velkého množství osob, se škoda na výše uvedeném podvodném jednání vyšplhala až na statisíce.

Výše uvedenému podvodnému jednání napomáhal fakt, že pachatel díky získaným přístupovým údajům vystupoval jako kamarád poškozených, tudíž poškození nebyli tolik obezřetní a díky neurčitému kódu bez uvedení nějaké finanční částky nemohli tušit, že se jedná o podvod. Proto bylo podvedených takové množství. Kdyby se jednalo o cizího člověka, který by oslovoval neznámé lidi s prosbou o zaslání nějakého kódu na jejich mobilní telefon, podvedených by bylo minimum. Dá se tedy říci, že pachatelé zjistili, že budou úspěšnější, když se stanou pro poškozeného důvěryhodnější a budou vystupovat jako kamarádi obětí.

Jak ve výše uvedeném případě postupovat? Obrana proti tomuto jednání je problematická. Pachatel využil velice sofistikovaný způsob podvodu. Věrohodně vystupoval jako kamarád poškozených přes účet jejich konkrétních kamarádů. Snad jediným způsobem, jak mohli poškození na podvodné jednání přijít, bylo zjistit si na internetu před odesláním bližší informace o zasílaném kódu. Díky těmto informacím by zjistili, že celá transakce není zdarma, což bylo v rozporu s tím, co tvrdil podvodník.

4.1.2. Podvodné vylákání finančních prostředků zasláním herních kupónů

Obdobný případ se stal koncem roku 2016, kdy pachatel využil důvěřivosti a touhy poškozené, získat levněji lístek na koncert jednoho známého zpěváka. Poškozená umístila na internet několik inzerátů včetně jednoho na sociální síti Facebook, kde jí kontaktovala osoba nacházející se na Slovensku s tím, že má k dispozici několik lístků na koncert, avšak lístky neposílá na dobírku, ale až po provedení platby. Pachatel však nechtěl poslat peníze na bankovní účet, jehož uživatel by mohl být snadno a rychle zjištěn, ale prostřednictvím herních kupónů v hodnotě nabízeného lístku na koncert. Poškozená tedy provedla nákup herních kupónů prostřednictvím platby ze svého bankovního účtu a kódy zakoupených herních kupónů napsala a poslala prostřednictvím facebookové zprávy pachateli. Ten od té doby přestal komunikovat a následně svůj facebookový profil přejmenoval a poté smazal. Následné šetření ztížil právě fakt, že si pachatel nenechal poslat peníze na bankovní účet, který je veden na jméno určité osoby, ale peníze získal jiným způsobem, ať už dobitím svého herního účtu, telefonního kreditu či herního či sázkového účtu, kde zjištění totožnosti podezřelého je složitější, v některých případech i téměř nemožné.

Pachatelům nahrává fakt, že profil na sociálních sítích si může anonymně vytvořit kdokoliv, umístit na profil libovolnou fotografii, kterou si stáhne kdekoliv z prostředí internetu a při podvodném jednání využívat další anonymní služby, které ztěžují následné jeho vypátrání. O to větší obezřetnost by měl člověk mít při jednání s neznámými osobami na internetu. Další konkrétní rady, jak alespoň částečně předcházet podvodnému jednání na internetu, uvedu v kapitole Metodické rady a možnosti pomoci.

Ve výše uvedeném případě pachatel zvolil platbu předem. V takových případech, kdy člověk neví nebo si není jist, kdo nějaké zboží nabízí a jaká je jeho spolehlivost, je lepší si nechat zaslat zboží na dobírku a po zjištění, že se jedná o podvod, transakci ve spolupráci s poštou a policií stornovat. Dále je vhodné například požadovat po prodejci fotografie lístků apod., protože je pravděpodobné, že lístky vůbec nedisponuje.

4.1.3. Seznámení s podvodníkem přes internetovou seznamku

Další zajímavý případ, který byl nakonec pro rozsáhlejší majetkovou trestnou činnost řešen jako trestný čin kriminální policií, započal podáním inzerátu na seznamce štěstí.cz.

Dle všeobecných podmínek poskytování služeb serveru štěstí.cz, je tato seznamka určena výhradně osobám starším 15 let, avšak při vyhledávání osob dle věku můžeme narazit i

na pár jedinců s vyplněným věkem 11 či 14 let. Případ, který následně budu popisovat, se stal plnoleté mladé slečně, ale může se klidně stát i mladistvé dívce, která se bude chtít v dobrém úmyslu vážně seznámit. (8)

Inzerát, který si na výše uvedené seznamce podal mladý muž z Prahy, vypadal pro mladé ženy chtivé seznámení na první pohled dobře. Mladý muž se v něm popsal jako dřívějšími vztahy zklamaný romantik, který konečně chce poznat dívku, která ho bude mít ráda a on ji a bude jí moci při západu slunce recitovat zamilované básně a vyznávat jí lásku. Na takovýto citově zabarvený inzerát se nechala nalákat jedna mladá žena z Prahy, taktéž se založeným profilem na serveru stesti.cz, která si přes tento server s mladým mužem po napsání několika vzkazů domluvila osobní schůzku. Žena souhlasila s první schůzkou rovnou u něho v bytě. Na schůzku přijela svým osobním automobilem. Po příchodu spolu začali konverzovat, popíjet alkohol a poté se odebrali do ložnice oddávat se milostným hrátkám. Poté oba usnuli. Vše do té doby vypadalo idylicky. Ráno se romantik vyjevil i jako pozorný gentleman, jelikož si prý všiml, že ženě nesvítí na vozidle jedna žárovka v předním světle a nabídl se, že ji vymění. Po snídani se oba rozloučili a spokojená mladá žena se chystala k odjezdu. V autě však zjistila, že jí nejen chybí autonavigace, ale v peněžence relativně vysoká finanční hotovost. Proto rovnou od milovníka jela na policejní služebnu, kde celou věc nahlásila. Po ztotožnění podezřelého bylo z dostupných evidencí policie zjištěno, že podvedená mladá žena nebyla jediná a jelikož se jednalo o déletrvající trestnou činnost s vyšší škodou, celou věc si převzala kriminální policie.

Ve výše uvedeném případě se jednalo o „jednoduššího“ jedince, který díky líbezným větám sbíral milostné zážitky a při té příležitosti se i finančně a majetkově obohacoval. K zakrývání své kriminální činnosti nevyvíjel žádnou výraznější námahu, kdy si například byt k pořádání schůzek půjčoval od svého kamaráda a bylo tím pádem pro policii snadné rychle na stopu podezřelého přijít a osobu ztotožnit.

Jelikož kromě sice dlouhotrvající, avšak jednotlivě drobné majetkové trestné činnosti, se v tomto případě vše ostatní zakládalo na dobrovolnosti, zakončil bych tento příběh poetickou hláškou, že „Není všechno zlato, co se třpytí“, a že je třeba si dávat větší pozor na podvodníky respektive na své věci i při seznamování s potenciální osudovou láskou.

4.1.4. Případ kybergroomingu 10 letého chlapce

Před pár lety se mi dostal do rukou případ jiného hrubého jednání, který sice naplňoval pouze skutkovou podstatu přestupku proti občanskému soužití dle § 49 odst. 1 písm. c) 200/1990 Sb., o přestupcích, ve znění účinném v době spáchání (nyní § 49 odst. 2 písm. d) zák.č. 200/1990 Sb., o přestupcích, ve znění pozdějších předpisů), avšak za jiných podmínek by mohl mít dalekosáhlé následky. Je zároveň typickým příkladem kybergroomingu.

Vše začalo kontaktováním 10 letého chlapce ze sociálně i finančně slabších poměrů. Chlapec žil v rodině s několika dalšími sourozenci a jen s jedním z rodičů - matkou – samoživitelkou, která navíc neměla žádné zkušenosti s výpočetní technikou, takže se nestarala ani o to, že její syn má profil na sociální síti Facebook, i když oficiálně si uživatel může na této síti založit profil až od 13 let. Na to, že si nezletilý s někým píše, přišla až jeho starší sestra, která si přečetla konverzaci s osobou, která vystupovala jako 16 letý chlapec a celou věc nahlásila policii, jelikož konverzace byla vedena ve stylu: „Líbí se ti kluci?“, „Vykouřil bys mi ho, kdybych ti poslal kredit?“. Šetřením bylo zjištěno, že se ve skutečnosti jednalo o 21 letého mladého muže, který byl za obdobné jednání již policií a následně správním orgánem v minulosti řešen. Vždy se jednalo „pouze“ o zaslání nevhodných návrhů, které nevyústilo v osobní schůzku. Ale jak jsem již uvedl, v případě někoho ne tak neškodného, by celá věc mohla dopadnout i tragicky.

V takových případech je rozumné mít jako rodič přehled o tom, kam jeho dítě chodí a s kým a jakým způsobem komunikuje.

4.1.5 Případ sextingu a kyberšikany 13 leté dívky

V roce 2015 se na mě obrátila matka nezletilé dcery s prosbou o pomoc. Dcera se totiž stala obětí jednak sextingu a jednak kyberšikany. V prvním případě v rámci komunikace se svým spolužákem, mu dívka poslala fotku svého poprsí. Spolužák však na základě této fotografie začal svou spolužačku vydírat a dožadoval se po ní pohlavního styku. Když mu nezletilá nevyhověla, poslal tuto fotografii dalším spolužákům ze třídy, kam oba docházeli i spolužákům do vedlejší třídy. Od nich se fotografie rozšířila prakticky po celé škole. Od té doby začaly chodit nezletilé různé urážlivé zprávy. Ty chodily dívce i předtím od její spolužačky, která si na ní zasedla a urážela jí díky skutečnosti, že rodina bojuje s rakovinou, tudíž nezapadala do modelu „dokonalé“ rodiny a něčím se tomuto modelu vymykala, což někteří jedinci nehodlají tolerovat, podobně jako když má ve třídě někdo starší model mobilního telefonu či oblečení nesplňující současné módní trendy. Spolužačka jí pomlouvala převážně na

sociální síti Facebook, ať už prostřednictvím soukromé komunikace nebo přidávala urážlivé texty na „zeď“, což viděly všechny osoby, které měla nezletilá i spolužačka v přátelích.

Jelikož se jednalo o 13 leté osoby, které v ČR ještě nejsou trestně odpovědné, věc se řešila ve spolupráci se školou a orgánem sociálně-právní ochrany dětí. Matka dokonce přemýšlela o přestěhování a přestupu dcery do jiné školy a zde si dávat větší pozor, aby tuto chybu už neopakovala.

Jak v tomto případě postupovat? Celou věc odstartovala zaslaná erotická fotografie. Je pochopitelné, že sexting je součástí zábavy mladých, ale nejen díky tomuto, ale i dalším případům je evidentní, že je to velice zneužitelný nástroj a některé činy (například rozeslání intimní fotografie) jsou již nevratné.

V případě kyberšikany je vhodné věc řešit ve vzájemné spolupráci školy a rodičů všech zúčastněných.

4.2. Ostatní tuzemské případy

Jak jsem již psal v teoretické části v podkapitole Kybergrooming, situace v tomto protiprávním jednání je alarmující. Ke zjištění míry závažnosti stačilo, aby si někteří novináři a kriminalisté vytvořili fiktivní profily nezletilých dívek, se kterými pak vstoupili do chatovacích místností, kdy během krátké doby je začaly oslovovat osoby nejdříve za účelem nezávazné lehce lechtivé konverzace a poté s žádostmi o zaslání erotických fotografií. V několika případech následně došlo k obvinění konkrétních osob a udělení podmíněných trestů za ohrožování výchovy dítěte a za zneužití dítěte k výrobě a šíření pornografie.

V první části bych se věnoval nejprve mediálně méně známým kriminálním případům zneužití. V další části budou popsány mediálně známé případy.

4.2.1. Zneužití nezletilých dívek

Takovýto způsob zneužívání přes internet bohužel není ojedinělý, jelikož prostředí internetu zajišťuje pachateli určitou dávku anonymity a díky velkému rozšíření sociálních sítí i velké množství potencionálních obětí. Uvedenému napomáhá i fakt, že velké množství obětí takového zneužívání zažívá stud a strach z reakce svého okolí, a proto se o něm zneužívaná osoba nikomu nesvěří a doufá, že zneužívání brzo skončí. K tomu většinou nedojde a ve většině případů se stupňuje. Takže nakonec zneužívané osobě stejně nic jiného nezbyde, než se s touto závažnou skutečností na někoho obrátit.

Na oficiálních stránkách Policie ČR (9) můžeme najít jeden typický příklad sextingu a kybergroomingu, který je bohužel reálný a má velký rozsah. Díky němu však můžeme názorně vidět, jaké praktiky, ať už psychologické či technické využívají groomerové při svých aktivitách.

Na výše uvedených stránkách začala jeden z případů internetového zneužívání v roce 2013 řešit královéhradecká kriminální policie díky tomu, že se jedna ze zneužívaných dívek obrátila nejdříve na své rodiče a ti poté na policii. Jednalo se o 14 letou dívku, kterou přes sociální síť kontaktoval tehdy 19 letý muž. Ten si na sociální síti Facebook vytvořil kromě jednoho svého profilu několik fiktivních profilů, většinou ve věku obtěžovaných dětí a následně si podle náhodně vybraných profilů na základě vzhledu resp. fotografií umístěných na těchto profilech, vybíral svoje oběti. Ty poté kontaktoval a nejdříve se v nich snažil vzbudit důvěru. Po nějaké době elektronické komunikace je požádal o zaslání fotografií s jejich intimními partiemi. Podle jejich reakce volil další postup. Buď nezletilá dívka souhlasila a zaslala mu své erotické fotografie, kdy tím pachatel obdržel silnou zbraň pro další zneužívání, či odmítla a pachatel dívce následně vyhrožoval, že jestli mu požadované fotografie nezašle, upraví fotografie v grafickém editoru, a to tak, že z internetu stáhne erotickou fotografii neznámé nahé dívky a vytvoří fotomontáž, kdy do fotografie překopíruje obličej obtěžované a následně fotografii rozešle jejím rodičům, kamarádům do školy apod. Už tato představa byla pro dívky tak stresující, že své erotické fotografie pachateli zaslaly. Takovým stylem zneužil 47 nezletilých a mladistvých dívek ve věku od 10 do 18 let, ať už ke zhotovení a vylákání erotických fotek, čímž se dopustil zneužití dítěte k výrobě a šíření pornografie nebo po získání fotografií a následném vydírání v některých případech i k nedobrovolnému pohlavnímu styku, čímž se dopustil sexuálního nátlaku, ohrožování výchovy dítěte a vydírání a pohlavního zneužití, za což mu hrozí až 12 let vězení. Uvedené číslo však není konečné a mohlo se jednat o zneužití až 400 dívek. Jak jsem již uvedl, velké množství poškozených má strach z reakce okolí a případné ostudy, která by se mohla snést na jejich hlavu, případně celé rodiny a způsobit tak posměch a narážky okolí, takže zneužití ani nenahlásí.

Obdobný případ řešili českolipští kriminalisté na přelomu roku 2010 a 2011, kdy třiadvacetiletý cizinec přes sociální sítě Facebook, ICQ a Skype oslovil několik stovek dívek ve věku 9-14 let, požadoval po nich, aby se fotily nahé a tyto fotky mu poté zaslaly. Se šesti z nich se sešel i osobně a pohlavně je zneužil. V dalších 49 případech se na zneužití připravoval. V tomto případě cizinci, který uměl velice dobře česky a své oběti si vybíral podle fotografií a informací, které o sobě dívky uvedly na internetu, hrozilo 8 let vězení. (10)

4.2.2. Případ Jiřího Kadrnožky

Jeden z již mediálně známějších případů se stal v roce 2007. V tu dobu 27 letý Jiří Kadrnožka pod přezdívkou Jirzin oslovoval uživatele chatu xchat v místnosti určené pro děti ve věku od 9 do 13 let s požadavkem, jestli se tam nachází mladá holka z Prahy nebo Nymburka, která by ho mohla uspokojit rukou. (11)

Tuto konverzaci sledoval redaktor MF DNES, který začal s výše jmenovaným komunikovat prostřednictvím založeného fiktivního profilu jako jedenáctiletá Tereza. Po konverzaci plné intimních návrhů Kadrnožka přemluvil „Terezu“ k osobní schůzce, kde už na něj čekali redaktoři MF DNES, kteří celou situaci zadokumentovali a předali policii. Následně Kadrnožkovi Obvodní soud v Praze 5 neuvěřil, že s dívkou konverzoval z nudy a myslel si, že si dívka vymýšlí ohledně svého věku a že je ve skutečnosti starší a za přípravu trestného činu pohlavního zneužívání mu udělil podmíněný dvouletý trest se čtyřletou zkušební lhůtou a zároveň mu nařídil ústavní sexuální léčbu.

4.2.3. Případ Pavla Hovorky

Další známý případ sextingu a kybergroomingu je kauza Pavla Hovorky. Ten nezačínal jako jiní, a to úpravou svého věku nebo vydáváním se za někoho jiného, ale vystupoval sám za sebe. Netajil ani svůj věk. Jediné, co si vymyslel, bylo jeho povolání. Vystupoval jako podnikatel a sponzor dětských domovů. Ve skutečnosti pracoval jako vrátný v jedné pražské tiskárně, kde i bydlel. Svoji první oběť nenalákal přes internet, ale prostřednictvím smyšlené soutěže s názvem „dítě VIP“, kdy jedno dítě z dětského domova v červenci roku 2005 vyhrálo 14 denní pobyt v Praze u Hovorky. Pobyt spočíval v trávení času s Hovorkou v jeho práci ve vrátnici, kde mělo dojít i ke zneužití chlapce. Údajně asi po 10 dnech sociální pracovníci chlapce vrátili kvůli blíže nespecifikovaným nevyhovujícím podmínkám zpět do domova. O zneužití se zprvu nevědělo, tudíž Hovorka mohl pokračovat ve svém protiprávním jednání, kdy změnil strategii a začal oslovovat nezletilé chlapce na internetu, kde si s nimi následně psal a i telefonoval. S některými se i sešel a nutil je k pohlavnímu styku. Když mu nechtěli vyhovět, vydíral je jejích nahými fotografiemi, které od nich předtím za úplatu vylákal. Dále jim vyhrožoval, že jestli mu nebudou po vůli, prozradí jejich homosexuální orientaci přátelům či rodině. Když se i přesto bránili, některé z nich i přes jejich odpor znásilnil. Za uvedené jednání Hovorkovi hrozilo až dvacet let vězení, avšak Městský soud zmírnil hrozící dvanáctiletý trest na osm let a následně Vrchní soud rozhodl o 6,5 letém nepodmíněném trestu odnětí svobody. (12)

4.3. Zahraniční kauzy

Výše uvedené příběhy sice nedopadly zrovna pozitivně, avšak nedošlo ke smrti zneužitých jako v následujících dvou případech, které taktéž chci využít jako odstrašující příklad, kam až může zajít ze začátku nevinná konverzace přes internet.

4.3.1. Případ Amandy Todd.

Kanaďanka Amanda Todd ve svých dvanácti letech chodila trávit svůj volný čas psaním na chatu. Psal se rok 1998. Na chatu se seznámila s neznámým mužem, který ji přesvědčil, aby mu ukázala svá ňadra. Amanda souhlasila. Jenže to neznámému muži nestačilo a chtěl víc. Chtěl jí vidět zcela obnaženou a když s tím Amanda nesouhlasila, začal ji vydírat, že její do půl těla nahou fotografii zveřejní, což následně udělal, jelikož se mu Amanda nepodvolila. Neznámý muž založil Facebookový profil, kam jako profilovou fotografii umístil již zmíněnou nahou fotografii Amandy. Ta se díky tomu rozšířila mezi spolužáky Amandy a lidmi z okolí a následkem toho začala být Amanda svým okolím šikanována. Nepomohlo ani přestěhování a změna školy. Nahá fotografie ji dostihla i tam. V září 2012 ještě umístila na sociální síti Youtube video, ve kterém se prostřednictvím krátkých vzkazů napsaných na několika papírech svěřovala se svým trápením. Jelikož ani po umístění tohoto videa na internet necítila od nikoho podporu, spáchala dne 10. 10. 2012 sebevraždu, kdy se ve svém domě oběsila. Viník, který vše odstartoval, nebyl nikdy dopaden. Byl pouze prověřován jeden dvaatřicetiletý muž, na jehož stopu přivedla policii skupina hackerů říkající si Anonymous. Ta ho vypátrala prostřednictvím jeho stop na internetu a zveřejnila jméno, datum narození a adresu. Kanadská policie se však k totožnosti muže poskytnuté od Anonymous, odmítla vyjádřit. A i kdyby to byl on, na její smrti nenese vinu jen on, ale i lidé z okolí Amandy a částečně i její rodiče a učitelé, kteří jí nepodali pomocnou ruku. Na začátku všeho však byla neopatrnost Amandy, kdy neznámému muži poskytla nástroj k jejímu vydírání a následné šikaně ze strany jejího okolí. (13), (14).

4.3.2. Ashleigh Hallová

Další tragický příběh se stal v Anglii v roce 2009. Tehdy si 17 letá studentka Ashleigh Hallová začala na sociální síti Facebook dopisovat s pohledným šestnáctiletým studentem Petem Cartwrightem. Ve skutečnosti se však jednalo o 32 letého Petera Chapmana, již známého sexuálního devianta. Ashleigh 25. října 2009 souhlasila s osobní schůzkou, na které záhy zjistila, že na místo nepřišel teenager z Facebooku, ale plešatý, nehezký, dospělý muž. Ten rafinovaně začal překvapené dívce tvrdit, že je otcem Peta Cartwrighta a že ho za ním odveze. Ve skutečnosti Ashleigh zavezl do pusté oblasti za město, kde ji znásilnil a poté svázal a zalepil

jí nos i ústa několika vrstvami lepící pásky, až se Ashleigh udusila. Bezvládné tělo pak pohodil do příkopu. V tomto případě byla policie úspěšná a soud vraha studentky odsoudil na 35 let. Matka Ashleigh Andrea Hallová se poté angažovala v informování široké veřejnosti před hrozbami sociálních sítí a vyzývala rodiče, aby nepouštěli své děti na sociální sítě, dokud nebudou plnoleté. (15), (16)

Osobně si nemyslím, že by uvedená situace vyplývala z věku zavražděné, ale spíše z minimální informovanosti a neopatrnosti, kdy Ashleigh udělala dvě zásadní chyby, včetně mylně informovaných svých rodičů, že bude přespávat u své kamarádky. Konkrétní rady, jak výše uvedeným situacím předcházet a jak postupovat, uvedu v následující kapitole.

5. Metodické rady a možnosti pomoci

V této kapitole bych se rád věnoval jednak prevenci před možným omezujícím, nevhodným či protiprávním jednáním, které na nás všechny číhá v prostředí internetu a jednak minimalizaci následků, když už k takovému jednání dojde. V úplném závěru této kapitoly bych popsal možnosti odborné pomoci.

Tyto rady jsou určeny nejen pro samotné žáky, učitele, rodiče, ale pro všechny, kteří se chtějí vyvarovat potencionálnímu nebezpečí, skrývajícímu se na internetu.

5.1. Zamezování rozvoje závislosti na internetu a sociálních sítích

Internet je dobrý sluha, ale špatný pán. Dobrý sluha může být internet v případě, že z něj budou děti čerpat informace k vypracování svých školních povinností, k rozšiřování svých znalostí a vědomostí. Nesmí se však aktivita na internetu zvrhnout ve hraní různých on-line her propagujících násilí (různé „střílečky“, „mlátičky“ apod.), sledování různých videí plných násilí a pornografie. Krom tohoto nebezpečí zde hrozí i to, že dítě zde bude z vlastní iniciativy trávit více času než v reálném světě a vybuduje si na internetu závislost. Dítě pak bude v době mimo počítač resp. internet nervózní, různé venkovní aktivity pro něj budou nudné a dítě bude dělat vše proto, aby se vrátilo domů a mohlo opět usednout k počítači.

Zábavu ve formě určitých online her, zábavných videí apod. nezavrhuji, může rodičům sloužit jako určitý druh odměny, avšak vhodné by bylo s touto odměnou nakládat s mírou a rozumem a hlavně ji mít pod kontrolou, ať už co se týče trvání, tak i co se týče náplně. Mít přehled o tom, na jaká videa se dítě dívá, jaké hry hraje, s kým si případně dopisuje. Cesta není dítěti něco zakazovat, ale dítě informovat a hlavně v něm vzbudit jistotu, že se na nás vychovatele či rodiče může kdykoliv s klidem beze strachu z nějakého postihu obrátit s žádostí o radu, když by se vyskytl jakýkoliv problém.

Jak jsem psal již výše, může zábava na internetu sloužit jako odměna, avšak v omezené míře a mít vše pod kontrolou, kdy je vhodné dětem najít jinou, lepší, alternativní zábavu, která bude mít nějaký pozitivní vliv na jejich rozvoj. Například výlety do přírody s nějakými doprovodnými činnostmi, kvízy, hrami, zlepšovat motorické schopnosti stavěním stavebnic apod.

5.2. Preventivní jednání, chování na internetu resp. na sociálních sítích

Prevence je jeden z nejdůležitějších postupů, jak předcházet různým nebezpečím na internetu resp. na sociálních sítích. Osvětu v tomto směru je potřeba šířit už od malých dětí, jelikož zahraniční průzkumy ukázaly, že i přes jednu z podmínek sociální sítě Facebook, že by uživatel měl být starší 13 let, tuto skutečnost nesplňuje plných 38 % uživatelů Facebooku, kteří jsou pod touto věkovou hranicí. Čtyři děti ze 100 jsou dokonce mladší šesti let. Nejpočetnější skupinu, a to z 80 %, tvoří děti ve věku od 13 do 16 let. (17)

5.3. Prevence

V následujících kapitolách uvedu jakým konkrétním oblastem by měli uživatelé internetu věnovat zvýšenou pozornost.

5.3.1. Opatrnost, obezřetnost

V dnešní době je převážně ve větších městech většina lidí nedůvěřivých. Není se čemu divit. Stačí, když si zapneme večerní zprávy či otevřeme internetový prohlížeč, kde se na nás začnou valit zprávy, kdo koho okradl, podvedl či zavraždil. O to více je zarážející fakt, jak velké množství lidí se nechá na internetu „napálit“. Ti, kteří si již prošli nějakou negativní zkušeností, začínají být obecně podezřívaví a nedůvěřiví, což je na jednu stranu dobře, že je již menší pravděpodobnost, že budou znovu podvedeni, na druhou stranu svojí nedůvěřivost promítají i do jiných oblastí svého života, o čemž jsem se sám přesvědčil na vlastní kůži, když jsem před lety hledal sportovní halu, kde jsem měl odehrát basketbalový zápas. Oslovil jsem ženu asi tak 50 letou, která zrovna venčila svého psa. Chtěl jsem se jí zeptat na cestu do oné sportovní haly. Stačilo, abych jí pozdravil „Dobrý večer“ a paní mě ani nenechala dokončit větu, skočila mi do řeči a řekla mi, že u sebe nemá žádné peníze a z místa urychleně odešla. Nutno připomenout, že jsem nebyl oblečen jako nějaký bezdomovec nebo konzument návykových látek. V tomhle případě nebyla tedy nedůvěřivost vůči cizím lidem na místě. Avšak v prostředí internetu a sociálních sítích je určitá obezřetnost potřebná tím spíš, když jednáme s cizími lidmi a jedná se o peníze nebo v některých případech i o lidský život.

Jak jsem již psal v úvodních kapitolách své práce, pachatelé používají velice sofistikované metody, jak své oběti podvést a být při tom co nejvíce důvěryhodní. A někdy jim k tomu stačí opravdu jen málo, pouze selský rozum.

Vybavuji si jednu kauzu, kdy se pachatelé velice jednoduchým způsobem dostávali na účet svých obětí „Můj Vodafone“, a to tak, že jim zavolali s nějakou výhodnou nabídkou na

volání či data a jak to operátoři například Vodafonu dělávají, zeptali se jich při prvním telefonátu na první a třetí číslici hesla. Když zavolali podruhé, zeptali se na druhou a čtvrtou. Tím získali přístup k jejich účtu a mohli s ním libovolně nakládat. Jednoduché, že? V takových a obdobných případech je dobré být velice opatrný, a když přesně nevíme, s kým hovoříme, nepodávat žádné důvěrné informace. Maximálně si vyslechnout nabídku s tím, že zbytek dokončíme sami nebo osobně na pobočce.

5.3.2. Bezpečnost hesel

S výše uvedeným souvisí bezpečnost jednak uchovávání a jednak tvorby hesel ke svým účtům respektive datům. Je vhodné si vytvářet složitější hesla s kombinací slov, čísel, a pokud to systém umožňuje, tak i interpunkcí. Dále je rozumné mít každý svůj účet zabezpečený jiným heslem. Mně osobně se stalo, že jsem měl zřízený účet na stránkách jednoho automobilového klubu. Ten měl své internetové stránky hůře zabezpečené, takže se zkušený hacker, který prolomil zabezpečení stránek, dostal k osobním datům tam uvedeným. A jelikož jsem měl stejné heslo pro přístup ke svému účtu na těchto stránkách jako ke svému emailovému účtu na serveru seznam.cz, útočník se dostal i do této schránky a tuto mi zrušil. Nerozumné je dále například napsat pin platební karty přímo na kartu či na lísteček založený v pouzdře společně s platební kartou.

5.3.3. Zasílání intimních fotografií

Další velkou chybou je zasílání svých erotických fotografií ať už svým kamarádům a v horším případě úplně cizím lidem, které neznáme a nikdy jsme osobně neviděli a vycházíme jen z konverzace, která je s druhou osobou vedena prostřednictvím elektronické komunikace. Tyto fotografie následně může zneužít nejen cizí osoba, ale i bývalý přítel po rozchodu či zhrzený milenec. Na toto doplatila bohužel velkými problémy spousta lidí a v některých případech takové nezodpovědné a neopatrné jednání skončilo i smrtí. Viz. v praktické části zmiňovaný případ Amandy Todd.

5.3.4. Uchovávání intimních fotografií

Dalším nebezpečím, které je spojené s pořizováním a následnou manipulací s intimními fotografiemi, je ukládání těchto fotografií na relativně zabezpečené internetové stránky, sociální sítě, či internetová úložiště. Schválně píšu pojem relativně, jelikož není problém pro zkušené hackery zabezpečení stránek prolomit, k datům se dostat a následně je včetně intimních fotografií zveřejnit, k čemuž došlo například v říjnu roku 2008, kdy se neznámému útočníkovi

podařilo obejít zabezpečení serveru Libimseti.cz a dostat se tak k 14417 intimním fotografiím z 1164 profilů, kde měli poškození tyto fotografie „uzamčeny“ heslem a nebyly volně přístupné veřejnosti. Dostupné měly být až po poskytnutí hesla uživatelem galerie. Následně hacker odcizené fotografie zveřejnil na několika internetových fórech. Odcizením a následným zveřejněním intimních fotografií se nevyhnuly ani zahraniční známé osobnosti, které umístily své nahé fotografie na virtuální úložiště iCloud. V roce 2014 neznámý útočník prolomil zabezpečení uvedeného úložiště a odcizené erotické fotografie celebrit umístil na internetové stránky 4chan a reddit.

Z výše uvedeného plyne doporučení, že když už si člověk chce uchovávat nějaké své intimní fotografie, měl by je ukládat na bezpečná úložiště, jako je například vlastní externí disk.

5.3.5. Pozor na falešné profily

Podobně obezřetný je třeba obecně být, když nás kontaktuje na sociální síti nějaká osoba, kterou osobně neznáme. Ve skutečnosti to totiž nemusí být ten/ta, za koho se vydává. Tato osoba může na svůj profil na internetu resp. sociální síti umístit libovolnou fotografii, uvádět nepravdivé informace o svém jménu, věku, bydlišti apod. V prostředí internetu a sociálních sítí prakticky nefunguje žádná kontrola, většina služeb je poskytována anonymně a záleží na každém, jaké informace o sobě vyplní. De facto jediná objektivní informace o uživateli, která se sice může, ale jen těžko, zmanipulovat, je jeho pasivní digitální stopa, kterou při svých aktivitách na internetu po sobě zanechává (více o digitální stopě v další podkapitole). A příklady z mé praxe i z mediálně známých případů upravování skutečností o věku, stavu apod. to jen potvrzují. Pachatelé, aby se s nimi jejich potencionální oběti vůbec začali bavit, si snižují věk na úroveň věku svých obětí, z internetu stahují fotografie nezletilých, za které se vydávají. Smyšlené je pak i jejich jméno. Ideální je s takovými cizími a podezřelými osobami vůbec nekomunikovat a nepřidávat si je do přátel. V případě jejich neodbytného naléhání si je úplně zablokovat.

Když už začneme s cizím člověkem komunikovat, není od věci si o této osobě zjistit nějaké bližší informace a pro začátek například prověřit jeho fotografii v některé na internetu dostupné vyhledávací službě, jako například tineye, vyhledávač obrázků google apod., kdy se může případně zjistit, jestli už tato fotografie nebyla někde na internetu umístěna a následně stažena. Dále když už s takovou osobou komunikujeme, můžeme jí vyzvat, aby se vyfotila s kouskem papíru, na který napíše námi vymyšlený vzkaz nebo jen slovo. Když se toto uskuteční okamžitě, minimalizuje se možnost, že by případný pachatel o toto požádal například

osobu, jejíž totožnost využil ke komunikaci s obětí. Další prověření osoby může být pomocí společné komunikace prostřednictvím videochatu například s využitím komunikačního programu Skype. Už jen samotnou výmluvu osoby na druhé straně, že nemůže uskutečnit videopřenos, lze považovat za podezřelou.

5.3.6. Sdělte dospělému o plánu setkání s neznámým

Další podcenění opatrnosti je neinformování dospělé osoby, jaké jsou naše plány s osobou z internetu, se kterou se chceme setkat. Například již zmiňovaná Ashleigh Hallová, když odcházela na schůzku s údajným sympatickým vrstevníkem, měla údajně napsat své matce, že ten den přespí u své kamarádky. Tento krok ji možná stál život.

Dnešní mobilní telefony zároveň umožňují pomocí gps a k tomu určené aplikace mapovat pohyb uživatele konkrétního mobilního telefonu, což by mohlo taktéž napomoci bezpečnějšímu průběhu setkání.

Mezi další velmi důležité preventivní zásady patří:

- nechodit s neznámou osobou na neznámá místa
- schůzku si případně domluvit na veřejném místě s velkou koncentrací lidí, například obchodní centra, náměstí apod.
- s neznámým člověkem nechodit do uzavřených prostor či nastupovat s ním do vozidla!

5.3.7. Na co si dávat pozor při zanechávání digitální stopy na internetu

Další zásadní věcí pro bezpečnost na internetu resp. sociálních sítích je mít pod kontrolou svojí digitální stoupu.

Digitální stopa je informace, kterou po sobě zanechává uživatel při používání internetu. Těchto stop je velké množství a dají se rozdělit podle jejich dostupnosti resp. obtížnosti vyhledání těchto informací, jelikož některé stopy jsou veřejné a snadno vyhledatelné, jiné jsou vyhledatelné s omezením, protože jsou přístupny pouze v rámci nějaké uzavřené skupiny, viditelné například až po provedení registrace, zadání přístupového hesla a například přidáním do přátel osoby na Facebooku, o které chceme něco zjistit. Dále jsou stopy zcela skryté, jako jsou například IP adresy, záznamy o navštívených serverech apod. Dále se digitální stopy mohou dělit podle způsobu zanechání stopy uživatelem na aktivní, které jsou vědomě zanechané a pasivní, což jsou stopy, které uživatel na internetu zanechává nezávisle na své vůli.

Mezi aktivní stopy, které jsou ve většině případů na internetu volně přístupné, patří například informace, které zveřejníme na svých profilech na sociálních sítích, příspěvky v diskuzních fórech, chatech, inzerátech, na internetu umístěné svoje fotografie, videa apod. Pasivní digitální stopy jsou pro většinu uživatelů internetu skryté, ale člověk, který je v dané věci znalý a zkušený, dokáže i některé tyto informace zjistit. Jedná se převážně o IP (Internet Protokol) adresu, což je unikátní číslo, které označuje a identifikuje počítačové zařízení v internetové a lokální síti, kdy podle této informace můžeme zjistit buď poskytovatele internetového připojení či zařízení v domácí nebo jiné vnitřní síti, jakými jsou například wifi zařízení či veškerá koncová zařízení (PC), která jsou k tomuto zařízení připojena. Tyto informace slouží jak při vystopování pachatelů trestných činností, tak i bohužel pro zkušené pachatele, kteří takto mohou vystopovat svoji oběť. K tomu je však potřeba buď nadstandardních dovedností v oblasti IT nebo zvláštní oprávnění, kterým disponuje Policie ČR.

Co se týče prevence rizikového chování na internetu a na sociálních sítích postačí, když si vysvětlíme několik pravidel ohledně zanechávání aktivních digitálních stop. Jedná se převážně o vkládání svých osobních fotografií, videí a osobních informací, které může pachatel následně zneužít. Například když člověk na svém veřejném, volně přístupném Facebookovém profilu umístí status, že si jede na 14 dnů užívat k moři. Zároveň má na svém profilu uvedeno, kde bydlí a ve své fotogalerii fotografie své osoby (například tzv. selfie), kdy za jeho zády je nějaký markantní objekt, podle kterého se dá určit pozice domu. Následně pachatel ví, že má 14 dnů na to, aby z domu sebral, co mohl a nikdo ho při tom nevyruší. Své o tom ví i známý anglický fotbalista John Terry, který na přelomu února a března 2017 umístil na internet svojí fotkou z francouzských Alp, kde byl lyžovat, kdy následně zloději vykradli jeho dům. (18)

K dalšímu přivedení na „vaši stopu“ napomůžete umístěním fotografie svého obličeje na profilovém obrázku umístěném na sociální síti. Alespoň co se týče oblíbené ruské sociální sítě V kontaktě (dále jen VK), což je ruská obdoba Facebooku založená v roce 2006 a čítající více než 370 milionů uživatelů. Jistý Rus Jegor Cvetkov tajně fotografoval lidi jedoucí v městské hromadné dopravě a tyto fotografie poté vložil do aplikace FindFace, která následně podle shodné podoby s profilovými fotografiemi na sociální síti VK vyhledala konkrétní osoby na právě výše uvedené sociální síti. Svůj projekt nazval příznačným názvem Your face is Big data. (19)

Digitální stopa však může naopak pomoci právě i při vystopování pachatelů protiprávního jednání na internetu, kdy však někteří sofistikovaní a zkušení pachatelé dokáží i

svojí pasivní digitální stopu úspěšně zamaskovat. Následné odhalení jejich stopy není nemožné, ale je velmi obtížné.

5.4. Jak řešit krizové situace, když k nim dojde?

Obecně se dá říci, že je lepší, když jsou na problém dva nebo více lidí, kteří nám můžou pomoci, poradit. Jak se říká „první na ráně“ jsou rodiče. Na jednu stranu své děti většinou dobře znají, na druhou se však jejich ratolesti občas stydí se jim svěřit se svými osobními věcmi, prožitky, intimními zážitky nebo jim to přijde přinejmenším trapné. Dalším omezením může být špatná technická znalost a vybavenost rodičů, kteří často nerozumí vymoženostem moderní techniky, nevědí, na jakém principu fungují sociální sítě apod. V dnešní době často ovládá výpočetní techniku lépe dítě než jeho rodič. Proto je vhodné kontaktovat někoho, kdo konkrétnímu případu nebo situaci rozumí, má o problému nějaké povědomí a s takovými případy již nějaké praktické zkušenosti. Existuje několik vyškolených pracovníků, které volající neznají. Tato skutečnost je pro volající dítě určitá výhoda, že se nemusí obávat ostudy, nějakých výčitek apod. a zároveň tito pracovníci dítěti můžou v dané věci poradit, jak by mělo dále postupovat, jak problém buď vyřešit, nebo na koho dalšího se s problémem obrátit.

V následujících podkapitolách se budu snažit popsat, na koho se konkrétně v jakém případě obrátit.

5.4.1. Jak postupovat v případě kyberšikany?

Dle metodického materiálu pro pedagogické pracovníky, který vytvořilo Národní centrum bezpečnějšího internetu (dále jen NCBI) v roce 2012, se kyberšikana a školní šikana prolínají. Proto nelze kyberšikanu u školních dětí šetřit odděleně, jako ojedinělou událost, ale je třeba ji řešit pouze jako jeden ukazatel rozvinuté šikany školní. Proto je potřeba v případě kyberšikany školních dětí podrobně prošetřit a poznat situaci ve třídě, ve které se toto elektronické násilí objevilo. V tomto případě je proto vhodné se obrátit na učitele, vychovatele, výchovného poradce či jiného pedagogického pracovníka, který problém bude řešit komplexně.

V případě, že by se dítě stydělo svěřit se svým problémem někomu, kdo ho zná, je možné se zkontaktovat s odborníky po telefonu nebo prostřednictvím online podpory. Možností koho kontaktovat je relativně velké množství. Dítě se může s konkrétním případem obrátit na Sdružení Linka bezpečí – Linka bezpečí 840111234, pomoconline.cz, Dětské krizové centrum – Linka důvěry 241484149, online ditekrize.cz, Národní centrum bezpečnějšího internetu – Horká linka, Nadace Naše dítě – Hotline, případně OSPOD v místě bydliště- sociální pracovníci

pro děti a mládež. Navazující psychologická pomoc dle místa bydliště – například Praha 1, 2 a 4, odborníci na školní šikanu a kyberšikanu www.pppppraha.cz, NCBI online na saferinternet.cz.

V případě kyberšikany mimo školní kolektiv je možné se taktéž obrátit telefonicky na výše uvedené linky či elektronicky na online podporu.

5.4.2. Jak postupovat v případě kybergroomingu?

Jelikož se groomeři zaměřují převážně na děti školního věku, je vhodné se s tímto obrátit buďto na rodiče nebo na nějakého pedagogického pracovníka, který může poradit co dělat dál, případně koho dále kontaktovat. Dále je možné se podobně jako v případě kyberšikany obrátit přímo na vyškolené pracovníky k tomu určených linek či online podpor nebo rovnou na Policii ČR.

Souběžně s obrácením se na pomoc dospělého či vyškoleného pracovníka je potřeba v případě podezřelého chování druhé osoby vyvinout vlastní aktivitu, a to:

a) Ukončit s osobou komunikaci
b) Nereagovat, neodpovídat, na další jeho vzkazy či výhrůžky
c) Blokovat útočníka
d) Pokud možno zajistit důkazy (screenshoty obrazovky, stažení fotek útočníka, zapsání případných dalších kontaktů jako je telefonní číslo, email apod., ..)
e) Požádat online podporu o odstranění závadného obsahu

Dále je třeba mít na paměti:

- Neřešení nebo přehlížení problému nic nevyřeší -> naopak může dojít k eskalaci problémů a zhoršení situace.
- Nereflektovat na výhrůžky typu: „Jestli mi nepošleš svoje další intimní fotografie, tak zveřejním ty, co už jsi poslal(a).
- Dále se nenechat vystrašit výhrůžkami typu: „Nikomu o mně neříkej nebo ublížím tobě nebo tvé rodině, vím kde bydlíš.“ apod. Útočník tak chce vzbudit u oběti strach (což se mu v mnoha případech i povede) a využít jej k lákání dalších intimních fotografií či vylákání ke schůzce a páchání dalšího zneužívání.

Aktivní by nemělo být jen dítě, ale oči otevřené by měl mít i rodič či pedagog, sledovat změny v chování dítěte a pokusit se zjistit, co se stalo (např. v případě Amandy Todd – okolí bez odpovídajícího zájmu).

5.5. Fungování podpor v praxi

V této podkapitole bych se rád věnoval popisu podpor, ať už online či telefonických, kdo je jejich provozovatelem a jak vlastně fungují.

5.5.1. Online podpory

Pro rozbor jsem si vybral online podporu Národní centrály bezpečnějšího internetu.

NCBI je neziskové nevládní sdružení založené v roce 2007, jehož cílem je, jak již samotný název napovídá, přispívat ke zvýšení bezpečnosti užívání internetu, moderních, informačních a komunikačních technologií, dále zvyšovat povědomí uživatelů o jejich kladech a možných nebezpečích, přispívat k osvojování etických norem v online prostředí, napomáhat předcházení a snižování možných sociálních rizik spojených s jejich užíváním. NCBI ve spolupráci se svými partnery pořádá různé konference, semináře, přednášky a školení zaměřené na oblast bezpečnějšího užívání internetu a prevenci internetové kriminality. (20)

Součástí NCBI je i online a telefonická podpora pro oběti rizikového chování a internetové kriminality.

Online podpora NCBI, která se nachází na stránkách onlinehelpline.cz resp. pomoconline.cz a je dostupná prostřednictvím odkazů umístěných jednak primárně na oficiálních stránkách NCBI, a to www.ncbi.cz či na stránkách přidruženého projektu saferinternet.cz, dále se odkazy na podporu nacházejí na stránkách www.bezpecne-online.cz, www.stoponline.cz, či www.seniorionline.cz.

Výše uvedená online helpline je jediná linka pomoci specializující se na problematiku zneužívání informačních technologií jako jsou internet, mobilní telefony, apod. Tato linka poskytuje pomoc v případech jako je kyberšikana, kybergrooming, stalking apod.

Oběti rizikového chování a internetové kriminality, ať už děti, mladiství, ale i dospělí a senioři, můžou pracovníka podpory kontaktovat jednak prostřednictvím formuláře, k němuž se dostanou na výše uvedených stránkách po kliknutí na možnost „Potřebuji pomoc“ v pravém horním rohu internetového prohlížeče či prostřednictvím zaslání emailu ze své emailové schránky na emailovou adresu helpline@saferinternet.cz.

Dotazy a žádosti o pomoc mohou zasílat 24 hodin denně, z důvodu ohraničené pracovní doby pracovníka NCBI jsou však zprávy či formuláře zaslané po 17 hodině akceptovány až následující den.

Svůj dotaz může kdokoliv zaslat anonymně, avšak uvedením svého jména či kontaktu na sebe se umožní odeslání odpovědi a zlepší se celkově vzájemná komunikace a tím i řešení konkrétního problému.

Dle pracovníka NCBI p. Palyzy přichází do centrály NCBI přibližně 40-50 dotazů měsíčně, buď prostřednictvím elektronických formulářů či formou emailové zprávy. Následně pracovník NCBI na tyto formuláře a emailové zprávy reaguje, a to tak, že poskytuje jednak rady právního charakteru, kdy kvalifikuje protiprávní jednání, zda a o jaký se jedná trestný čin či přestupek či jiné jednání a na koho se v té dané konkrétní věci obrátit, tak i co se týče pomoci technického směru, kdy radí, jak zajistit případné důkazy proti podezřelému, jak se zbavit škodlivého softwaru apod.

Problém s kontaktováním online podpory na FB.

Kromě kontaktování výše uvedených online podpor je možné se obrátit přímo na online podporu konkrétní sociální sítě, na které ke kyberšikaně dochází. Průběh komunikace a nahlašování nějakého problému však sebou může nést určitá úskalí. Například komunikace se zaměstnanci sociální sítě Facebook je velmi obtížná, komunikace probíhá ve většině případů prostřednictvím nejrůznějších typů formulářů umístěných na Facebooku. Nejbližší centrála Facebooku se nachází v Dublinu v Irsku.

Problematická blokace.

Facebook je vybaven formuláři pro blokaci závadného obsahu. Účinnost této blokace je však různá, kdy k zablokování nevhodného obsahu dojde v rozpětí několika hodin až několika měsíců. Vhodnější je proto nahlášení závadného obsahu prostřednictvím k tomu určených organizací jako například internethotline.cz nebo k blokaci využít také Online poradnu v rámci projektu E-Bezpečí na internetové adrese napisnam.cz.

Zkušenosti NCBI s kontaktováním online podpory na FB.

Dle pracovníka NCBI v Praze p. Palyzy je v případě relevantního hlášení zaslaného prostřednictvím online formuláře, který je přeložen i do českého jazyka, tento následně zaslán do vyhodnocovacího centra, které údajně sídlí v Indii, kdy reakční doba je zpravidla do tří pracovních dnů. Tato doba se však výrazně zkracuje podáním opakovaného či skupinového hlášení, kdy se následná reakční doba může zkrátit až na hodiny. Vyhodnocovací centrum může zablokovat jednotlivé nevhodné fotografie či v případě právě kyberšikany či kybergroomingu celé profily.

Další on-line řešení kyberšikany.

Dále je možné se dle intenzity a závažnosti kyberšikany obrátit na online technickou pomoc. V současné době jsou v ČR dvě. Jedna nevládní: Horká linka na horkalinka.net a jedna provozovaná Policií ČR: Horká linka Policie ČR (formulář na aplikace.policie.cz/hotline/).

Před kontaktováním online podpory, kdy by následně mělo dojít k zablokování útočníka, je vhodné zajistit důkazy o nevhodném chování či protiprávním jednání. V případě komunikace na sociální síti Facebook je buď možné vytvořit screeny obrazovky s danou komunikací či si stáhnout komunikaci v sekci archiv.

5.5.2. Telefonní linky

Kontaktovat podporu NCBI může kdokoliv nejen prostřednictvím online formuláře, ale pro lepší a okamžitou zpětnou vazbu i prostřednictvím telefonního hovoru.

Hovor přijímá vyškolený pracovník NCBI, který stejně jako v případě kontaktování elektronickou formou poskytuje právní a technické rady, kdy výhoda telefonního hovoru je v tom, že zkušený pracovník může poskytnout online podporu a návod, jak problém převážně technického charakteru rovnou vyřešit.

6. Závěr

Jako jednu ze základních priorit v boji proti nástrahám na internetu shledávám v lepší informovanosti nejen dětí, ale i rodičů a pedagogických pracovníků. Dětem je třeba vysvětlit, že to není jen o tom zapnout počítač, tablet či se na internet připojit z mobilního telefonu, a že tím vstoupí do obrovského pohádkového světa téměř neomezených možností. Že podobně jako v pohádkách na ně mohou v prostředí internetu číhat různé nástrahy a zlé bytosti. A že na rozdíl od toho pohádkového světa v našem reálném světě ne vždy vítězí dobro nad zlem. Aby zlo nezvítězilo, je třeba, aby se rodiče i přes nedostatek svého drahocenného času přinutili k většímu zájmu o své děti a měli větší přehled o jejich aktivitách na internetu.

Cílem práce bylo na základě zpracování dat z konkrétních kriminálních případů a několika výzkumů vytvořit přehled existujících rizik spojených s používáním sociálních sítí dětmi a mládeží. Tento přehled byl pak podkladem pro připravení metodických doporučení jak pro prevenci, tak i pro řešení konkrétních krizových situací.

Svou práci jsem pojal komplexně, abych obsáhl co nejvíce situací a kroků pro co nejlepší informovanost dětí prostřednictvím rodičů či pedagogických pracovníků. Dále jsem pro celistvost okrajově zmínil i některá další důležitá rizika „číhající“ v prostředí internetu i mimo sociální sítě jako například phishing či rhybaření. Ve své práci jsem se snažil poukázat na aktuální rizika hrozící nejen dětem na internetu resp. sociálních sítích. K tomu je však nutno podotknout, že se metody a prostředky pachatelů v prostředí internetu neustále mění a vyvíjejí, a že je potřeba se neustále aktivně o těchto nových trendech informovat a zjišťovat, jak se proti nim účinně bránit.

Byl bych proto rád, aby tato práce zlepšila podvědomí o rizicích, které na všechny a převážně na děti mohou v prostředí internetu resp. sociálních sítí čekat, ale spíše všechny zúčastněné navedla tím správným směrem, a to obecně bezpečnějšímu používání internetu a aktivnímu zájmu o tento problém. A jestli má práce napomůže k odvrácení byť jen jednoho reálného nebezpečí, které by jakémukoliv dítěti hrozilo, pak mé snažení nebylo zbytečné.

7. Seznam použitých informačních zdrojů

1. LUKÁŠOVÁ K., PACÁK R., MAŠKOVÁ A. *Výchova k bezpečnému a etickému užívání internetu: Metodický materiál pro pedagogické pracovníky* [online]. Národní centrum bezpečnějšího internetu, 2012 [cit. 10. února 2017]. Dostupné na WWW: http://www.ncbi.cz/category/6-metodiky-ucebni-materialy?download=49

2. Sociální sítě. *Aktuálně.cz* [online]. 3. červenec 2011 [cit. 5. února 2017]. Dostupné na WWW: https://www.aktualne.cz/wiki/veda-a-technika/socialni-site/r~i:wiki:1456/

3. Facebook. *Wikipedie* [online]. 27. března 2017 [cit. 28. března 2017]. Dostupné na WWW: https://cs.wikipedia.org/wiki/Facebook

4. Badoo. *Wikipedie* [online]. 23. května 2016 [Citace: 28. březen 2017]. Dostupné na WWW: https://cs.wikipedia.org/wiki/Badoo

5. KRČMÁŘOVÁ, B. *Děti a online rizika.* 1. vyd. Praha : Sdružení linka bezpečí, 2012. ISBN: 978-80-904920-2-8.

6. Elektrošoky jako trest pro závislé na intenrnetu mají v Číně skončit. *Novinky.cz* [online]. 15. ledna 2017 [cit. 28. března 2017]. Dostupné na WWW: https://www.novinky.cz/internet-a-pc/426491-elektrosoky-jako-trest-pro-zavisle-na-internetu-maji-v-cine-skoncit.html

7. HINDUJA, S., PATCHIN, J.W. *Bullying Beyond the Schoolyard: preventing and responding to cyberbullying.* Thousand Oaks, California : Corwin Press, 2009. ISBN: 978-1-4129-6688-7.

8. Všeobecné podmínky poskytování služeb štěstí.cz. *Štěstí.cz.* [online]. 1. červen 2006 [cit. 10. duben 2017]. Dostupné na WWW: https://www.stesti.cz/pravidla/

9. JEŽKOVÁ, I. Otřesný případ zneužívání přes internet. *Policie.cz* [online]. 15. července 2015 [cit. 7. února 2017]. Dostupné na WWW: www.policie.cz/clanek/otresny-pripad-zneuzivani-pres-internet.aspx

10. Cizinec zneužil šest dívek, stovky školaček zkontaktoval přes internet. *iDnes.cz* [online]. 10. ledna 2011 [cit. 7. února 2017]. Dostupné na WWW: zpravy.idnes.cz/cizinec-zneuzil-šest-divek-stovky-skolacek-zkontaktoval-pres-internet-1ar-/krimi.aspx?=A110110_123202_krimi_zep

11. Rande s lolitou vyneslo mladému muži podmínku. *iDnes.cz* [online]. 5. dubna 2007. [cit. 7. února 2017]. Dostupné na WWW: zpravy.idnes.cz/rande-s-lolitou-vyneslo-mlademu-muzi-podminku-fq1-/krimi.aspx?c=A070405_130802_krimi_anv

12. Zneužil přes dvacet chlapců, dostal osm let. *Novinky.cz.* [online] 5. února 2009 [cit. 10. dubna 2017]. Dostupné na WWW: http://www.novinky.cz/clanek/160547-zneuzil-pres-dvacet-chlapcu-dostal-osm-let.html

13. Patnáctiletá Amanda: Uštvali ji k smrti. *Zena.cz.* [online] 14. listopadu 2012 [cit. 10. dubna 2017]. Dostupné na WWW: http://www.zena.cz/rodina/patnáctiletá-amanda-ustvali-ji-k-smrti

14. Canadian teen found dead weeks after posting wrenching YouTube video detailing bullying. *Fox News* [online]. 12. října 2012 [cit. 10. dubna 2017]. Dostupné na WWW: www.foxnews.com/world/2012/10/12/canadien-teen-found-dead-weeks-after-posting-wrenching-youtube-video-detailing.html

15. ŠVAMBERK, A. Sedmnáctiletou obět si našel na facebooku, znásilnil ji a zavražidl. *Novinky.cz* [online]. 9. března 2010 [cit. 2. února 2017]. Dostupné na WWW: www.novinky.cz/zahranicni/evropa/194196-sedmnactiletou-obet-si-nasel-na-facebooku-znasilnil-ji-a-zavrazdil.html

16. STOKES, P. Ashleigh Hall: One mistake cost teenager her life. *The Telegraph* [online]. 8. března 2010 [cit. 2. února 2017]. Dostupné na WWW: www.telegraph.co.uk/news/uknews/crime/7398085/Ashleigh-Hall-one-mistake-cost-teenager-her-life.html.

17. Rizika sociálních sítí a co by děti měly vědět [online]. Národní centrum bezpečnějšího internetu, 2014. Dostupné na WWW: http://www.ncbi.cz/category/6-metodiky-ucebni-materialy?download=85

18. Hvězdě Chelsea vykradli dům, teď tvrďák poslal lapkům vzkaz: Nehrajte si se mnou. *Sport.cz* [online]. 7. března 2017 [cit. 10. března 2017]. Dostupné na WWW: https://www.sport.cz/fotbal/premier-league/clanek/862110-hvezde-chelsea-vykradli-dum-ted-tvrdak-poslal-lapkum-vzkaz-nehrajte-si-se-mnou.html.

19. BARET, D. Fotograf tajně vyfotil lidi a porovnal to s jejich snímky na sociální síti. Co objevil? *Reflex* [online] 22. prosince 2016 [cit. 8. ledna 2017]. Dostupné na WWW:

http://www.reflex.cz/clanek/fotogalerie/76676/fotograf-tajne-vyfotil-lidi-a-porovnal-to-s-jejich-snimky-na-socialni-siti-co-objevil.html.

20. Národní centrum bezpečnějšího internetu [online]. 2012 [cit. 10. dubna 2017]. Dostupné na WWW: www.ncbi.cz.